

The Increasing Role of Bring Your Own Device (BYOD) in CXM – Trends, Challenges, and Opportunities

THINSCALE This document has been licensed to ThinScale

David Rickard, Vice President
Deepanshu Agarwal, Senior Analyst

Contents

Introduction	03
Understanding the BYOD operating model	04
Why organizations are considering the BYOD model	05
Major challenges in implementing BYOD and their solutions	09
Selecting the right BYOD implementation partner	13
The role of BYOD in an organization's Environment, Social, and Governance (ESG) strategy	14
Case study	16
Conclusion	17

Introduction

Over the past few years, the business landscape has rapidly shifted to a digital-first environment, with enterprises focusing on technologies including advanced analytics, intelligent automation, and Artificial Intelligence (AI), and customers shifting to digital channels such as chat, email, and social media. The COVID-19 pandemic has further expedited this transition and transformed enterprise operating models, with employees now accessing corporate data through their personal handheld devices or laptops outside the corporate network.

This increasing adoption of the Bring Your Own Device (BYOD) operating model can be attributed to multiple factors:

- The availability of a more secure and safe architecture for BYOD solutions
- Increased margin pressures on providers and enterprises forcing organizations to opt for all possible cost-saving measures
- The increased need for flexibility and scalability amid a dynamic market; COVID-19 driven lockdowns and restrictions are making enterprises and providers evaluate non-traditional methods to onboard employees/agents in the shortest time
- A focus on superior Employee Experience (EX) by providing employees the option to work on a user-friendly interface of their choice using BYOD solutions; high employee satisfaction can improve Customer Experience (CX) (To understand how EX positively impacts CX, read our viewpoint Delivering Superior Experiences: How Positive Agent Experience Amplifies Customer Experience)
- Increased acceptance of the Work At Home Agent (WAHA) delivery model, which has increased enterprises' willingness to use BYOD solutions to enable working from home

For this research, we interviewed Chief Technology Officers (CTOs), Chief Information Officers (CIOs), Chief Security Officers (CSOs), and Chief Information Security Officers (CISOs) of leading enterprises and providers who shared their views on the benefits of using a BYOD model, including:

- Significant cost reductions due to lower capital investment and shipping costs, as employees work on their own devices
- Improved agent experience, as agents do not have to wait for a corporate device to start working and can get onboarded quickly
- More flexibility and scalability due to faster and easier technology deployment

In this viewpoint, we study the BYOD model with a focus on laptops and computers (also known as the Bring Your Own Computer or BYOC model). We examine:

- The benefits of implementing BYOD solutions
- Current macroeconomic trends around BYOD adoption
- Outlook for BYOD and the COVID-19 pandemic's impact
- Challenges in BYOD implementation
- Criteria for selecting the right partner in BYOD implementation
- The role of BYOD in an organization's ESG strategy

Understanding the BYOD operating model

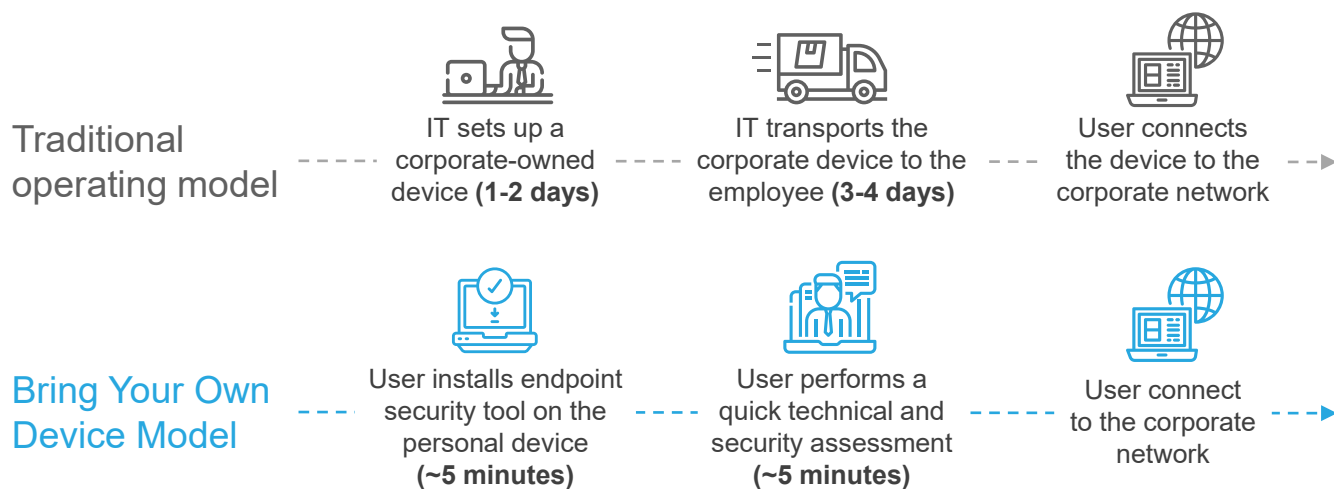
BYOD is an operating model in which employees use their personal devices, such as laptops, desktops, or tablets, to work and access enterprise data anytime, anywhere. Companies that have implemented BYOD policies allow their employees to work on their own devices instead of using devices that the company owns and manages.

The exhibit below outlines the contrast between a traditional operating model and a BYOD model.

EXHIBIT 1

A traditional model vs a BYOD model

Source: Everest Group (2022)



Why organizations are considering a BYOD model

Everest Group take

With advances in consumer electronics and organizations going global, operating models are changing continuously. Many employees today prefer to work on the device of their choice. Moreover, with supply shortages due to lockdowns and the silicon chip crisis and the need for a faster onboarding process, some organizations are choosing to use employees' personal devices to maintain business continuity. Accompanying benefits such as higher agent satisfaction and lower capital costs further drive the adoption of BYOD solutions.

Challenges that enterprises and providers face with the traditional operating model

Organizations are facing multiple challenges in serving their customers in the current environment, which has further suffered due to the pandemic. These problems include:

- Providers and enterprises are facing significant margin pressures due to increased competition and an economic downturn in the pandemic's wake. Many organizations, especially those with a seasonal business and high employee turnover, face huge device losses when employees do not return corporate devices. This is a bigger problem when new hires are shipped the devices, but they do not join the organization, making the organization incur logistics costs and probable device loss in case they keep the device. The exhibit 2 below highlights this challenge through an example.

EXHIBIT 2

The exhibit below highlights this challenge through an example

Source: Everest Group (2022)



A BPO company needs to hire 1,000 agents.



The company recruits 1,500 agents for training, as it faces ~35% agent attrition before the joining date.

Does not include cost of logistics team, IT resources, or attrition

500 agents exit before the joining date. The company recalls the devices that it had shipped to them.



The company ships devices costing US\$400 per device to all its 1,500 agents, incurring an additional logistics cost of US\$50 per device. The total cost incurred is US\$675,000.



Only 80% of the devices are recovered. At a return logistics cost US\$50 per device, the total cost incurred is US\$20,000. In addition, the BPO suffers a capital loss of US\$40,000 for the unrecovered devices.



The total capital loss and device shipping costs to and from agents adds up to US\$135,000.

- The pandemic-induced market uncertainty is pushing organizations to become more agile in their operations. They need to increase the pace of employee/agent onboarding to scale operations and maintain business continuity
- Severe shortage of new devices due to the silicon chip crisis and multiple restrictions due to the pandemic have made it difficult to provide equipment to onboard new employees in a short period
- Organizations with seasonal businesses find it difficult to procure and ship devices quickly when ramping up during the peak demand period and recover the devices when ramping down afterward
- There is lower employee/agent satisfaction because of dissatisfaction with the tools that some enterprises and providers offer. This dissatisfaction could be on account of multiple devices (personal and corporate-issued) that an employee may have to carry or the lack of familiarity with the device and/or operating system. Low EX translates into poor interactions with both internal and external stakeholders, which might ultimately affect CX, resulting in dissatisfied customers and negative attrition
- CX is the key differentiator among competitors, driving the demand for superior customer experience. Hence, finding the right talent is critical for maintaining target customer service levels and overall CX. However, traditional operating models may restrict an organization's talent pool to regions where hardware is readily available or where shipping devices is relatively easy. These challenges can lead to a longer recruitment cycle and exorbitant logistics costs, making it difficult to hire quality talent from across the globe

How BYOD tackles these challenges

BYOD addresses the above-listed challenges effectively as it:

- **Offers long-term cost savings:** The BYOD model allows employees to use their own devices, thereby saving enterprise costs for initial device purchase, logistics costs to ship the device, and ongoing technical support costs in case of repair or exchange. It also reduces the cost of employee downtime by saving the time required for shipping devices if any technical repair is needed. Employees can get the device repaired nearby, making the repairing process less complicated
- **Delivers agility in operations:** Amid the pandemic, many countries imposed restrictions on working from an office, and it became challenging for employers to send new devices or repair devices of employees in non-office locations with all the restrictions and lockdowns in place. Even after the pandemic, employees may prefer to work from home for at least a few days of their working week and may not live close to a corporate office. A BYOD model in the WAHA setting allows employers to quickly onboard employees globally despite lockdowns and bring them up to speed through their personal devices, making it easier for the organization to scale. Furthermore, with many organizations considering the gig workforce as their potential operating model, BYOD can play a vital role in its successful implementation. A gig model can cut an organization's cost of recruiting full-time employees and shipping them new devices. BYOD can provide a secure interface for gig workers to use their personal devices for corporate work, resulting in improved scalability of operations
- **Mitigates supply issues:** A BYOD model addresses the silicon chip shortage by eliminating the need to purchase new devices for new hires and allowing them to work on their personal devices. This also reduces the duplication of devices for an employee as they do not have to carry separate device for work and personal use

- **Facilitates quick agent onboarding:** Organizations can quickly implement BYOD solutions on agents' personal devices without incurring any capital expenditure. Thus, BYOD enables organizations to quickly onboard new agents, which is particularly beneficial for seasonal businesses that need to hire part-time agents for short durations during peak demand
- **Offers higher employee satisfaction:** As BYOD solutions allow employees to choose their user interface and allow them to work with a device that they are familiar with, employees are more productive right from the start. This head-start reduces the onboarding time and can make employees productive from the first day. A BYOD model eliminates the need to carry two devices, making it easier for employees and supporting flexible work arrangements. These advantages result in higher employee satisfaction, reduced employee attrition, and improved productivity
- **Enables superior CX delivery:** A BYOD model allows organizations to hire quality talent quickly and globally to provide best-in-class CX. Additionally, as the time and cost to ship devices are saved, organizations can pass the accompanying benefits to their customers

Additionally, some organizations in the software and technology sectors are leveraging BYOD as a beta-testing ground before releasing their products in the market. Employees act as beta-testers, and they can highlight the issues and changes required in a product after using it on their personal devices. This helps better understand the end customer's needs and make improvements to the final product.

The exhibit below highlights the benefits of BYOD adoption for organizations.

EXHIBIT 3

Benefits of BYOD implementation

Source: Everest Group (2022)

	Offers long-term cost savings
	Delivers agility in operations
	Mitigates supply issues
	Facilitates quick agent onboarding
	Offers higher employee satisfaction
	Enables superior CX delivery



Despite the above benefits of the BYOD operating model, it had few takers in the market initially due to corporate data and information security concerns. But market sentiment has changed with the growing recognition among service providers and enterprises that a secure BYOD model can be

achieved. The availability of solutions providing security at par with corporate devices and widespread BYOD adoption in various industries, including regulated sectors such as healthcare and BFSI, have increased BYOD's prominence further.

Macroeconomic trends vis-à-vis BYOD adoption

BYOD solutions have experienced increased adoption across industries and geographies over the past couple of years, with the pandemic expediting the adoption. Below we look at some of the key trends across industries and geographies driving this change.

- Industry trends:** Industries such as telecom, media, retail, travel, logistics, and transportation are increasingly adopting BYOD, especially for handheld devices. The BFSI sector is also adopting BYOD solutions for front-end processes such as customer onboarding, account opening/closure, and loan processing, but adoption continues to be at an early stage in other highly regulated sectors, such as healthcare and the public sector. Although Health Insurance Portability and Accountability Act (HIPAA) and other standards-compliant solutions aim to protect patient/confidential information, data safety concerns remain in a BYOD delivery model due to the information's highly sensitive nature
- Geographic trends:** Developed economies such as the US, the UK, and continental Europe are leading the shift to a BYOD solutions model. Employees in these geographies have multiple devices at home, easy access to technical support, robust internet coverage, and better accessibility to the technology market to purchase new devices, if required. To avoid managing or toggling between personal devices and corporate-issued devices and use one's choice of interface, employees in economically advanced countries prefer the BYOD model. However, countries such as Germany and Spain face legislative issues vis-à-vis the BYOD model. The EU and individual governments within it must balance the need for user privacy with corporate security requirements to allow enterprises to enable a successful BYOD model

Future outlook for BYOD

The BYOD model seems to have a promising future, with increased adoption among various industries globally, including regulated sectors, due to the following reasons:

- The pandemic has expedited BYOD adoption due to the emergence of WAHA and gig workforce operating models, and industry leaders are recognizing that safe and secure BYOD operations are possible. The increased need for scalability and flexibility in operations is pushing organizations to achieve faster onboarding processes, driving the implementation of BYOD solutions. Additionally, organizations are letting their employees use their personal devices to allow user-friendly interfaces and have reduced employee downtime
- BYOD solutions have become more secure than in the past and comply with standards such as the General Data Protection Regulation (GDPR), Payment Card Industry Data Security Standards (PCI DSS), and Health Insurance Portability and Accountability Act (HIPAA). In fact, data security in a BYOD model is today equivalent to devices that corporate IT teams own and manage
- Although organizations are slow to adopt the BYOD model due to investments already made in corporate devices, new and upcoming firms are expected to promote BYOD growth. Furthermore, organizations facing device losses due to low recovery rates are expected to transition to the BYOD model to save shipping and capital (device loss) costs

Major challenges in implementing BYOD and their solutions

Everest Group take

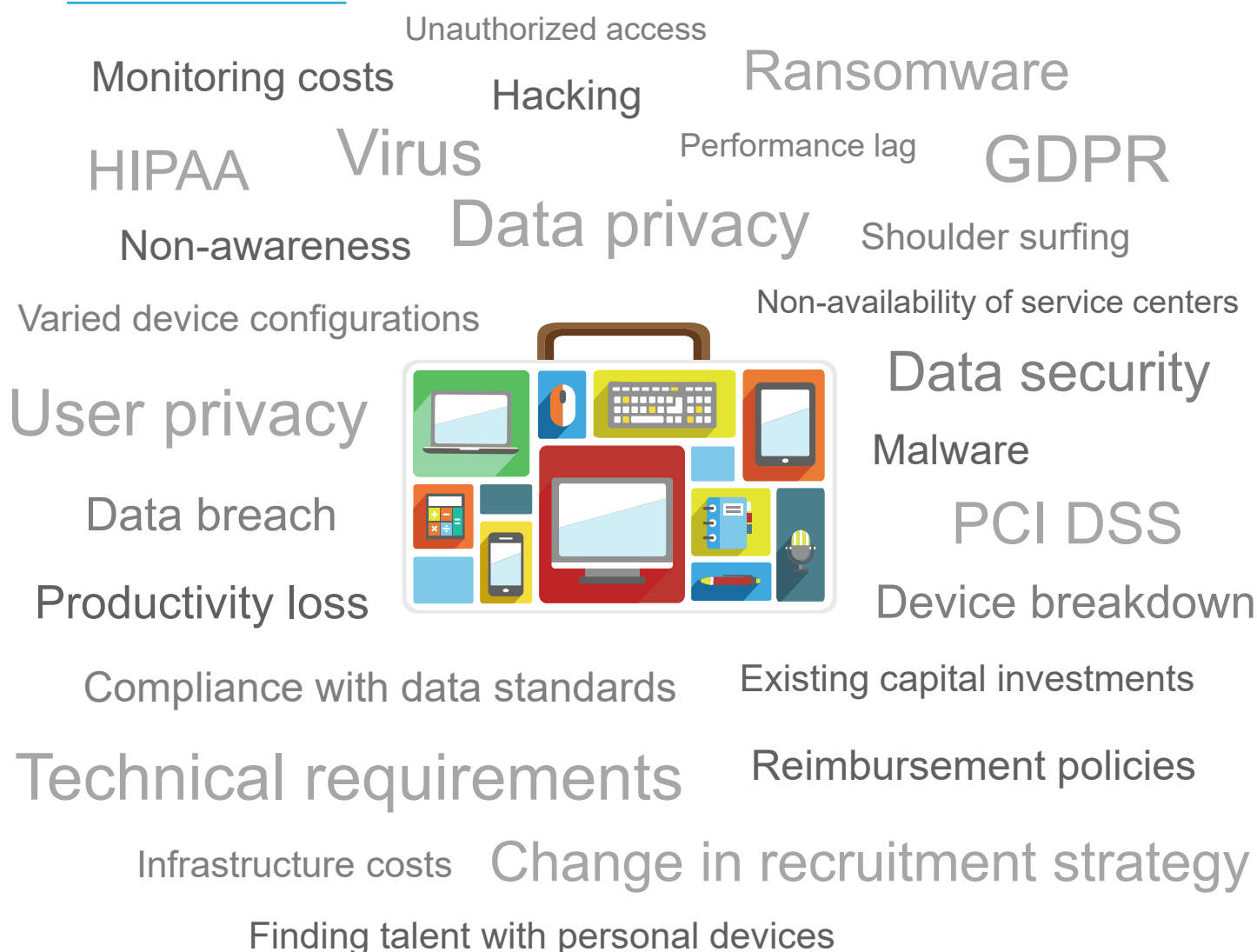
Allowing employees to work on their personal computers can benefit both the employer and the employee. However, despite the benefits, organizational leaders continue to be skeptical of the BYOD model. To achieve success, organizations should work to address the concerns of their senior management.

We asked senior leaders, including CTOs, CIOs, CSOs, and CISOs, at enterprises and provider firms to list their key challenges and concerns with the BYOD model. The word cloud below depicts their concerns.


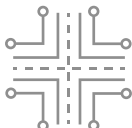

EXHIBIT 4

Senior leaders' concerns with the BYOD model




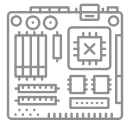
Source: Everest Group (2022)





Below we take a closer look at these challenges, along with their solutions:

	Challenges	Mitigation plan
Data security and privacy risks 	<p>Organizations are concerned about possible data breaches due to lost or stolen devices. They fear employees plugging in unauthorized USB drives to hack into the network or copy confidential data from the corporate network to their personal networks. Personal devices are more prone to malware and viruses, compounding the risk of data leakage. Although some of these challenges can be addressed through desktop virtualization (VDI or DaaS), the endpoint remains vulnerable. It is vital in many industries, especially regulated sectors, that solutions comply with security standards such as GDPR, HIPAA, and PCI, which can pose challenges to using personal devices.</p>	<p>Organizations should select a BYOD solution that complies with PCI, GDPR, and HIPAA standards. To prevent data breaches due to lost/stolen devices or unauthorized access by employees exiting the organization, the solution should be capable of remotely denying corporate access and uninstalling the application from the device after an employee's exit or in cases of unauthorized access. The solution should temporarily create a restriction layer that completely locks the user out of the underlying operating system. It should deny any use of USB drives that can potentially hack into the system and the corporate network. Preventing employees from copying, pasting, or saving any data from a secure session to their personal devices can further prevent any data leakages. Additionally, the presence of quick security and technical requirement checks within the solution can ensure that the device follows the requisite standards before each session.</p>
Increased security infrastructure and monitoring costs 	<p>Finance teams are concerned that the cost of implementing best-in-class security parameters, security architecture, and monitoring tools for BYOD solutions might outweigh the cost savings from corporate devices, making the transition to the BYOD model unappealing.</p>	<p>Organizations should partner with a BYOD service provider that can offer SaaS solutions with a secure architecture that complies with international data security standards and eliminates the need to separately invest a significant amount in security infrastructure, thereby reducing the cost to deploy. For corporate-issued devices, the device recovery rate is always less than 100% when an employee leaves the business and can lead to significant losses for any large-scale employer. Many new recruits leave during the training period, resulting in additional shipping costs without any financial gain if the device is returned. Therefore, logistics have become a major factor in the BYOD business case, which eliminates the logistics component and, in fact, increases agility in hiring, recruitment, and scaling. It is thus likely to have a more positive commercial impact.</p>
User privacy concerns 	<p>Some users may have privacy concerns due to the perception that their personal devices will be constantly monitored even when not in use for work-related tasks. Employees might demand from their employers the right to use their devices without any visibility into what they use their devices for.</p>	<p>The BYOD solution should completely segregate the device's personal use from its corporate use. It needs to ensure that no employee's private data is monitored to allay any privacy concerns.</p>

	Challenges	Mitigation plan
Lack of awareness among senior management about BYOD solutions' security capabilities 	<p>The senior leadership at many organizations still lacks awareness about BYOD solutions' security capabilities, including BYOD solutions compliant with GDPR, PCI, and HIPAA. In our study, few respondents indicated confusion between the WAHA and BYOD models and noted challenges and concerns related to the WAHA delivery model (as opposed to BYOD), such as shoulder surfing and clicking pictures of confidential data, which can happen with both corporate-owned devices as well as personal devices.</p>	<p>With leading BPOs starting to adopt the BYOD model, these solutions are increasingly gaining traction. The available BYOD solutions in the market can provide secure frameworks at par with IT-controlled corporate devices. Organizations should look for BYOD partners that can provide informational content around the security of BYOD solutions, in terms of Proof of Concept (POC) or case studies, from both regulated and unregulated sectors.</p>
Difficulty in meeting technical requirements in personal devices 	<p>To meet security standards, IT teams define the minimum technical requirements for personal devices. If an employee's personal device falls below that requirement, they will have to purchase a new device with a higher specification, which requires investment. An employee may be unwilling to do so unless the company pays for it. Also, the assessment of devices from a technical and safety perspective might increase the recruitment cycle's duration.</p>	<p>For new hires, organizations should prioritize a solution that provides an endpoint check to remotely inspect personal devices at the earliest point in the hiring process and again during onboarding, to determine the device's performance requirements. For existing employees, if a device does not meet the required specifications, organizations may choose to offer a corporate-owned device or provide support to purchase a new device or upgrade the existing one.</p>
The need to better understand changes needed in the recruitment strategy 	<p>Talent acquisition teams and other stakeholders are concerned they do not fully understand the changes required in their recruitment strategies to accommodate the shift to a BYOD model.</p>	<p>A BYOD model does not require any change in recruitment strategies. On the contrary, it can easily work with existing methods and even simplify these, as organizations do not need to prepare corporate-owned devices and ship them to employees. The only additional requirement in the existing hiring process is to validate the device capabilities required to operate in a BYOD environment, which can be done during the interview process. By selecting the right BYOD solution, an organization can onboard an employee in a few minutes, once the device is approved for BYOD use, by installing an endpoint security tool. Moreover, when an employee leaves the organization, the firm can easily block the employee's access to corporate servers by remotely uninstalling the BYOD solution, saving the hassle of managing device recoveries.</p>

	Challenges	Mitigation plan
Performance lag 	<p>Senior leaders across organizations are skeptical about the performance of BYOD solutions. They believe that during memory-intensive tasks, virtualized desktops will not be able to perform properly, and employees might face lag. These drawbacks will hamper employee productivity, and they may get frustrated due to slow performance.</p>	<p>A BYOD model can outperform the specifications of an employee's personal device by using cloud computing. With a virtual office environment set up on high-performance servers, employees can easily use their lower specification devices to access corporate servers through the cloud with all computing done on the server, reducing the need for high computing power in personal devices. Additionally, organizations can utilize a resource distribution tool that allows an organization's IT team to monitor the use of resources at an individual level and redistribute computing power where it is needed.</p>
Varied device configurations 	<p>Due to device variances (both hardware and software) among employees, IT teams may face difficulties in providing support to employees should an issue arise. This will either impact employees' productivity or force them to seek technical support from the original equipment manufacturer, which may be slower than internal IT teams and increase downtime.</p>	<p>Typically, any potential increase in downtime due to technical support requirements is offset by a shorter agent onboarding time in using a new device. Moreover, as employees are familiar with their personal devices, they typically require less IT support on a daily basis. Organizations should select a BYOD solution that sits as a secure layer on top of the device's hardware and software, creating a uniform and IT-controlled user experience. The IT team can, thus, continue to support end users and provide a consistent user experience to all employees.</p>
Finding the talent pool with the required personal devices 	<p>A few BPO service providers expressed concerns regarding the availability of employees with personal devices that can be used for corporate work.</p>	<p>In today's digital era, people have easy and significant access to personal devices such as laptops and computers. Therefore, organizations can find the right talent pool anywhere across the world. Also, as a BYOD model leverages the principle of cloud computing, people with lower device specifications can convert their devices for corporate work, eliminating the need to hire people with high-specification computers or laptops. In unusual circumstances, if someone with the right skill set does not have a personal device, organizations can provide them an incentive to purchase one locally. The company can provide them a monthly allowance or have an agreement in place to return the device allowance should they leave the organization before a specified period.</p>
Lack of hardware availability in local markets 	<p>In the event of a fault in the device or a complete breakdown, employees who cannot get support from the IT team may need to seek external support to get a device repaired or to purchase a new device. In the WAHA model, many employees work from a remote location with limited access to repair shops or retail stores for PCs and laptops. Any delay in repairing or procuring a new device will increase employee downtime and reduce their productivity.</p>	<p>Typically, it is easier and cheaper to repair or purchase a device locally than to wait for a corporate device to be delivered. But, in case of limited access to retail stores, companies can incentivize employees to use online markets that provide quick pick-and-drop facilities. This additional cost is offset by the savings made by reducing the IT team's workload. In exigencies, employees can still send their devices to their companies, as the hardware is largely the same as that of corporate-owned devices.</p>

	Challenges	Mitigation plan
Existing capital investments in corporate-owned devices 	<p>Many organizations have already invested heavily in corporate-owned devices. Shifting to BYOD solutions might make their existing investments futile.</p>	<p>Every organization needs to purchase new machines regularly. Therefore, when existing devices' life cycles end, organizations can shift to a BYOD model. In the meantime, they can make a gradual transition to a BYOD solution. Additionally, instead of discarding devices that have already been purchased, organizations can use these as a replacement when an agent faces a technical difficulty or an irreparable damage to their personal device, thereby reducing downtime.</p>
Development of reimbursement policies 	<p>Employees may ask for a partial or full reimbursement for using their personal devices for work purposes, citing that the employer would have otherwise invested some amount in procuring a device for them. In such cases, the HR function will need to draft a reimbursement policy that safeguards the interests of both the employer and the employee.</p>	<p>Although reimbursement policies might be needed for agents using their personal devices, organizations can become more competitive when hiring talent by paying more to candidate for working on their personal devices. This additional employee cost can be offset by the significant savings made in terms of capital expenditure on corporate-owned devices.</p>

Selecting the right partner to implement BYOD

Everest Group take

BYOD solutions address multiple challenges that organizations face today and provide several benefits to both employers and employees. To implement them successfully, organizations must evaluate and select the right technology partner to meet their technical and security parameters.

BYOD solutions need to be fully secure and comply with industry regulations, especially for regulated sectors such as healthcare and BFSI. For safe and secure implementation, organizations should select a BYOD partner that can:

- Provide a total endpoint security solution:** The BYOD solution should prevent any unauthorized access to data by means such as copying, pasting, or clicking screenshots of official information and transferring it to a personal network. The endpoint security solution should completely isolate corporate and personal data and block any unauthorized plug-ins of USB drives. It should turn the device into a fully secure corporate device and temporarily disable access to personal data until the employee is active on a corporate server
- Offer an easy-and-fast remote BYOD implementation:** Employees should not be required to bring their personal devices to the office to set them up for corporate use. The solution should provide a fast, simple, and easy remote conversion of a personal device into a BYOD device
- Detect attempts to tamper with the device:** The solution should be capable of flagging any potential attempt by an employee to tamper with the device or gain privileged access to the device bypassing IT restrictions. It should notify the IT team immediately and secure the device remotely if such incidents occur

- **Safeguard users' privacy:** Although a BYOD solution should provide access to a user's device to control corporate data access and prevent potential breaches, it should also protect employee privacy. The solution should ensure that personal data remains separate from corporate data and that the IT team does not monitor employees' activities, credentials, or keystrokes on a personal network
- **Ensure compliance with HIPAA, GDPR, and PCI standards:** Many industries require compliance with stringent international standards, such as GDPR, PCI, and HIPAA. Therefore, a BYOD solution should help organizations, especially those operating in highly regulated industries that store and process personal customer data, achieve these compliances
- **Provide Multi-Factor Authentication (MFA) and Single Sign-On (SSO):** The BYOD partner should be able to provide an SSO facility to save employees from credential fatigue and reduce the possibility of data breaches due to improper management or storage of multiple credentials. To prevent password leakages, MFA options such as a One Time Password (OTP) on phone or email, security questions, and fingerprint scan should be implemented
- **Offer access through secured Virtual Desktop Infrastructure (VDI) or Desktop-as-a-Service (DaaS):** A VDI or DaaS architecture is preferred to implement a BYOD model. Accessing a corporate interface over the cloud keeps the personal and corporate use of a device separate. A VDI environment is like virtually accessing a desktop in an office through a personal device. Therefore, it allows the organization to have better control over the device and prevents the transfer of viruses and malware from a personal device to the corporate network
- **Restrict use from certain locations:** An organization should be able to safeguard confidential data and information by having the option to restrict employees from accessing a corporate network from locations such as public places that have higher chances of data breaches
- **Provide device management with remote wipe capabilities:** An endpoint security solution should be able to remotely wipe any corporate applications or information in case of a potential data breach if a device is lost or stolen
- **Protect from malware, phishing attacks, and other cybersecurity risks:** The BYOD solution should be able to prevent phishing attacks and safeguard corporate information from malware, ransomware, or viruses. The solution should continuously monitor any cyber threats to the device by using firewalls, antiviruses, and other security tools. Confidential information such as passwords, credit card details, and personal data gets stolen via keylogging and screen-scraping applications. Therefore, the BYOD solution should be able to restrict such applications

The role of BYOD in an organization's ESG strategy

Everest Group take

A well-managed ESG strategy can act as a catalyst for an organization to capture new opportunities and business, potentially outperform others, and stay ahead of the market. A BYOD model offers benefits to employees and the employer but is also beneficial to the environment by reducing the duplication of devices. Therefore, a BYOD model plays a vital role in ESG, and organizations should consider its role carefully when forming their ESG strategies.

Among the many benefits that it offers, the BYOD model's positive impact on organizations' ESG mandates is undeniable, as exhibited below.

EXHIBIT 5

BYOD benefits vis-à-vis ESG

Source: Everest Group (2022)

- Reduces device duplication
- Saves to-and-fro transportation of corporate devices
- Reduces e-waste

Lowers carbon footprint

Strengthens ESG initiatives



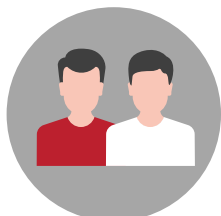
Implementing a BYOD solution benefits the environment and, therefore, plays a key role in an organization's ESG strategy. In a traditional operating model, employees toggle between a personal device and a corporate-issued device to separate their use of work and home devices. This segregation also means doubling the raw materials required to make the devices and incurring logistics costs to transport them from manufacturers to retailers or end users. Furthermore, more than one device consumes power daily. Manufacturing a PC requires about 1.8 tons of raw materials and 240 kilograms of fossil fuels, which translates to a significant figure for the entire workforce.

However, with BYOD, employees can use the same device for both corporate and personal use, which eliminates device duplication. Additionally, as employees undergo rapid onboarding on their own devices, the company saves on device shipping costs. The model also saves on subsequent to-and-fro transportation of devices in case of a device breakdown, as employees can get their devices repaired at nearby centers. Furthermore, BYOD also makes it easier to manage contractual workers, especially those hired for short durations to cover peak periods.

The BYOD model not only supports organizations in achieving their sustainability goals, but also enables them to capture new market opportunities. As customers become environmentally and socially conscious, they look at their engagements with organizations as more than just supplier-customer relationships. They want to be associated with organizations that operate without negatively affecting the environment. BYOD solutions can help organizations reduce their carbon footprints and emerge as model organizations for existing and potential customers. Also, organizations can claim carbon credits and launch ESG bonds in the market to monetize the positive impact of implementing BYOD on the environment.

Case study

How iQor ensured business continuity via a BYOD model to address accelerated demand for WAHA



Client overview

Challenges

iQor is a managed services provider of customer engagement and technology-enabled BPO solutions, with over 35,000 employees in nine countries. The company serves various industries, including financial services firms and leading wireless carriers.

iQor faced the following challenges during the COVID-19-driven lockdowns:

- Agents were no longer able to access on-site thin clients, or computers that run from resources stored on a central server, due to COVID-19 lockdowns
- The purchase of new machines was not reliable due to pandemic-related supply chain and logistical challenges. Lockdowns also made the delivery and distribution of corporate devices difficult

Thus, the company wanted a solution that could help it achieve the following objectives:

- Allow employees to access their VMware Horizon environment securely from the comfort of their homes
- Have a swift onboarding process, with reduced costs and increased scalability, while meeting the required security and compliance norms
- Overcome supply and logistics costs issues



Solution

A total endpoint security software in a VDI environment to provide a secure BYOD model

- The solution is a software-only application installed on an agent's PC or laptop. It converts an unmanaged PC into a fully managed secure thin client device when needed
- Organizations can manage their entire remote device estate using a single management platform with a single administrative console
- The software temporarily disables access to underlying OS, preventing unauthorized access to the organization's data, such as copying data from the corporate server to personal storage



Results

The agent onboarding period reduced from days and hours to minutes and the organization experienced a host of other benefits:

- Equal security across on-premise and BYOD models
- One-click device capability validation to get agents assessed and onboarded within minutes, with little or no handholding from IT
- Same level of control for organizations over their on-site devices and the BYOD software; agents have complete privacy once logged out from corporate servers
- Ability to manage the entire remote device estate via a single management platform

Conclusion

With the increasing virtualization of workspaces and globalization of the talent pool, the BYOD model looks at a promising future. Many organizations have started focusing on ESG agendas, and BYOD solutions have become the stepping-stone in this journey due to their positive impact on the environment.

Although some industries, especially those in regulated sectors such as healthcare and BFSI, are slow to adopt BYOD due to data security and privacy concerns, advances in the BYOD architecture can mitigate most of these concerns. To achieve success with their BYOD implementations, organizations should select the right partner that can provide best-in-class technology and security controls to provide an unparalleled experience to both employers and employees.

Everest Group is a research firm focused on strategic IT, business services, engineering services, and sourcing. Our research also covers the technologies that power those processes and functions and the related talent trends and strategies. Our clients include leading global companies, service and technology providers, and investors. Clients use our services to guide their journeys to maximize operational and financial performance, transform experiences, and realize high-impact business outcomes. Details and in-depth content are available at www.everestgrp.com.

This study was funded, in part, by ThinScale



For more information about Everest Group, please contact:

+1-214-451-3000

info@everestgrp.com



For more information about this topic please contact the author(s):

David Rickard, Vice President

david.rickard@everestgrp.com

Deepanshu Agarwal, Senior Analyst

deepanshu.agarwal@everestgrp.com