مجله مدیریت اطلاعات سلامت
سال هفدهم/ شماره دوم/ خرداد و تیر ۱۳۹۹

Published by *Vesnu Publications*
DOI: 10.22122/him.v17i2.4121

سیاست‌گذاری برای به کارگیری رویکرد Bring your own device در همه‌گیری کووید ۱۹: بیان دیدگاه

مریم جهانبخش[۱]، مصطفی امینی رارانی[۲]، شهرام طهماسبیان[۳]، معصومه شهبازی[۴]

بیان دیدگاه

دریافت مقاله: ۱۳۹۸/۱۲/۱۴ پذیرش مقاله: ۱۳۹۹/۲/۳۱ تاریخ انتشار: ۱۳۹۹/۳/۱۵

ارجاع: جهانبخش مریم، امینی رارانی مصطفی، طهماسبیان شهرام، شهبازی معصومه. **سیاست‌گذاری برای به کارگیری رویکرد Bring your own device در همه‌گیری کووید ۱۹: بیان دیدگاه.** مدیریت اطلاعات سلامت ۱۳۹۹؛ ۱۷ (۲): ۸۹-۸۷

مقدمه

در آغاز سال ۲۰۲۰ میلادی، بیماری کووید ۱۹ جهان را درگیر همه‌گیری نمود و در ابعاد مختلف اقتصادی، اجتماعی، پزشکی و سیاسی چالش‌های بی‌شماری را در دنیا ایجاد کرد. یکی از مشکلات عمده جوامع برای کنترل شیوع کرونا ویروس، استمرار فعالیت‌های اجتماعی و اقتصادی و انجام وظایف شغلی افراد در طی دوران قرنطینه بود. دورکاری به عنوان یکی از مهم‌ترین سیاست‌های پیشگیری و کنترل کووید ۱۹ توسط کشورهای مختلف به کار گرفته شد. همچنین، بسیاری از افراد شاغل ترجیح می‌دادند وظایف شغلی‌شان را به صورت دورکاری انجام دهند. در چنین شرایطی، اهمیت به کارگیری رویکردهایی مانند BYOD (Bring your own device) و در واقع، استفاده از تجهیزات الکترونیک شخصی برای انجام وظایف شغلی بیش از هر زمان دیگری آشکار شد. سازمان‌ها برای به کارگیری رویکرد BYOD و بهره بردن از مزایای آن، مستلزم سیاست‌گذاری صحیح و اجرای دقیق آن هستند. در این نوشتار تلاش شده است چگونگی به کارگیری سیاست استفاده از BYOD تبیین شود. از دیدگاه ما، مهم‌ترین شاخص‌هایی که می‌تواند در سیاستگذاری برای به کارگیری BYOD مد نظر قرار گیرد، شامل تصمیم‌گیری صحیح در انتخاب و اجرا، زیرساخت‌های فنی، ارتباط مستمر، آموزش کارکنان، پروتکل‌های امنیت و محرمانگی، توافق‌نامه بین کارکنان و سازمان و استفاده از خدمات ذخیره‌سازی ابری می‌باشد.

شرح دیدگاه

خوشبختانه وجود فن‌آوری‌های اطلاعاتی در دنیای امروز، امکان تداوم زندگی حرفه‌ای و خصوصی به صورت مجازی را ممکن ساخته و موجب شده است که بسیاری از افراد بتوانند وظایف شغلی خود را در هر مکانی فارغ از مکان سازمانی انجام دهند (۱). بر همین اساس، بسیاری از سازمان‌ها و کارفرمایان به منظور تداوم فعالیت‌های اقتصادی خود در دوران شیوع ویروس کرونا، ترجیح می‌دهند که کارمندانشان به دورکاری بپردازند (۲).

دورکاری با استفاده از BYOD در کنار مزایای حاصله، دارای چالش‌های بسیاری است که از مهم‌ترین آن‌ها می‌توان به مخاطرات امنیت اطلاعات اشاره نمود. بنابراین، تدوین سیاست‌ها و قوانین مناسب سازمانی و همچنین، اجرای مطلوب آن‌ها اهمیت بسیاری دارد. از جمله این که در سیاست‌گذاری در خصوص BYOD، باید به موضوعاتی همچون کارمندان مجاز، برنامه‌های کاربردی مورد استفاده بر روی دستگاه‌های شخصی، حقوق سازمان در دسترسی به داده‌های شخصی افراد، پشتیبانی و امنیت دستگاه‌های مذکور و در نهایت، چگونگی کاهش خطرات مرتبط با این رویکرد توجه داشت (۲). هنگام اجرای سیاست BYOD، هیچ‌گاه نمی‌توان تمامی موضوعات محتمل را مشخص نمود، اما موضوعات زیر از جمله مهم‌ترین مواردی است که شایسته است به هنگام اجرای این رویکرد مورد توجه کارفرمایان و سازمان‌ها قرار گیرد:

در سیاست‌گذاری برای اجرای BYOD، باید به تصمیم‌گیری صحیح در حداقل سه زمینه کلیدی مشتمل بر «امکان‌پذیری مالی، قانونی و فرهنگی استفاده از BYOD در سازمان، چگونگی رفع مشکلات امنیتی احتمالی حین اجرا و وجود پوشش‌های بیمه‌ای برای رفع خسارات وارده به داده‌ها و ابزارهای شخصی کارکنان» توجه نمود (۱).

استفاده از BYOD همچون دیگر انواع فن‌آوری‌ها نیازمند «زیرساخت فن‌آوری اطلاعات» مناسب به ویژه در بعد فنی می‌باشد. فراهم کردن پهنای باند مناسب، امکان حفظ تعداد زیادی از اتصالات کاربران به سرورها و امکان اجرای نرم‌افزارهای مانیتورینگ شبکه به منظور کنترل افراد، از جمله زیرساخت‌های

مقاله حاصل پایان نامه کارشناسی ارشد به شماره ۳۹۸۷۹۹ می‌باشد که با حمایت دانشگاه علوم پزشکی اصفهان انجام شده است.

۱- استادیار، مدیریت اطلاعات سلامت، مرکز تحقیقات فن‌آوری اطلاعات سلامت و گروه مدیریت فن‌آوری اطلاعات سلامت، دانشکده مدیریت و اطلاع‌رسانی پزشکی، دانشگاه علوم پزشکی اصفهان، اصفهان، ایران
۲- استادیار، سیاست‌گذاری سلامت، مرکز تحقیقات مدیریت و اقتصاد سلامت، دانشگاه علوم پزشکی اصفهان، اصفهان، ایران
۳- استادیار، انفورماتیک پزشکی، گروه زیست فن‌آوری پزشکی، دانشکده پزشکی، دانشگاه علوم پزشکی شهرکرد، شهرکرد، ایران
۴- دانشجوی کارشناسی ارشد، فن‌آوری اطلاعات سلامت، گروه مدیریت فن‌آوری اطلاعات سلامت، دانشکده مدیریت و اطلاع‌رسانی پزشکی، دانشگاه علوم پزشکی اصفهان، اصفهان، ایران
نویسنده طرف مکاتبه: معصومه شهبازی؛ دانشجوی کارشناسی ارشد، فن‌آوری اطلاعات سلامت، دانشگاه علوم پزشکی اصفهان، اصفهان، ایران
Email: m.shahbazi995@gmail.com

فنی است که به عنوان پیش‌نیازهای سیاست‌گذاری در این حوزه به شمار می‌رود. این موارد علاوه بر این که می‌تواند خطرات امنیتی را کنترل نماید، در ایجاد ارتباطی بی‌نقص برای کاربران و تداوم مناسب فعالیت‌های کاری نیز دارای اهمیت است (۱).

به علت احتمال ایجاد مخاطرات امنیتی در زمان استفاده از BYOD و همچنین، اهمیت تأمین امنیت اطلاعات شخصی کارکنان و نیز مشتریان، سازمان‌ها باید از وجود «پروتکل‌های حفظ امنیت و محرمانگی» مانند ساز و کارهای امنیتی مختلف همچون استفاده از ویروس‌یاب‌ها، فایروال‌ها، پتچ‌های امنیتی و ابزارهای رمزگذاری دستگاه‌ها، درگاه‌های رمزگذاری شده ایمن یا استفاده از شبکه‌های خصوصی مجازی کاملاً به‌روز و کافی اطمینان حاصل کنند (۳، ۲).

علاوه بر این، به سازمان‌ها پیشنهاد می‌شود از «سرویس‌های معتبر ابری» استفاده نمایند تا اطلاعات سازمان به جای ذخیره در ابزارهای شخصی کارکنان، در سرویس‌های ابری قابل اطمینان ذخیره شود (۴) و در صورت سرقت دستگاه شخصی یا دسترسی غیر مجاز به آن، امنیت اطلاعات سازمان در معرض خطر قرار نگیرد. لازم است که سرویس‌های ذخیره‌سازی ابری و شرایط عقد قرارداد آن‌ها نیز پیش از استفاده توسط بخش فن‌آوری اطلاعات سازمان به طور کامل بررسی و تأیید گردد.

کارکنان از ارکان مهم به کارگیری رویکرد BYOD در سازمان به شمار می‌روند و بر همین اساس، وجود «توافقنامه‌ای رسمی بین سازمان و کارکنان» اهمیت دارد. ابعاد این توافقنامه باید کارکنان را ملزم به انجام صحیح وظایف کاری و نیز پایبندی و پاسخگویی نسبت به سیاست‌های حریم خصوصی و محرمانگی سازمان نماید. این توافقنامه می‌تواند از وقوع بسیاری از مشکلات حقوقی و شکایت‌های آتی پیشگیری کند (۱).

«حفظ استمرار ارتباط با کارکنان»، از موارد مهم به کارگیری این رویکرد است. کارکنان طی استفاده از BYOD به ویژه در هنگام دورکاری، باید از وجود مسیرهای ارتباطی مناسب با سازمان اطمینان خاطر داشته باشند. وجود دستورالعمل‌های صریح و دقیق، شاه‌کلید ارتباطی در این زمینه است. علاوه بر این، به کارگیری شیوه‌های ارتباط از راه دور همچون ویدئو کنفرانس، می‌تواند منجر به حمایت و جلب رضایت کارکنان شود (۵).

«آموزش» همواره از ابعاد مهم اجرای یک فن‌آوری به شمار می‌رود. بنابراین، آموزش به کارکنان در هنگام استفاده از BYOD لازم و ضروری است (۵، ۲). کارکنان باید مطلع باشند که چگونه رمز عبور پیش‌فرض روتر بی‌سیم خود را تغییر دهند، از شبکه‌های بی‌سیم عمومی استفاده نکنند، برنامه‌های مورد نیازشان را از فروشگاه‌های معتبر تهیه کنند (۶)، از کلیک بر روی لینک‌های ناآشنا و باز کردن ایمیل‌های نامشخص پرهیز نمایند و از چاپ کردن اطلاعات حساس سازمانی و ارسال آن‌ها به ایمیل و حساب‌های شخصی نامشخص نیز جلوگیری نمایند (۳).

نتیجه‌گیری

رویکرد BYOD به واسطه ترغیب کارکنان یک سازمان به استفاده از دستگاه‌های همراه شخصی (مانند گوشی‌های هوشمند، تبلت یا آی‌پد و سایر موارد مرتبط) در انجام وظایف شغلی، می‌تواند برای دورکاری در همه‌گیری‌هایی همچون کووید ۱۹ به کار گرفته شود. در نتیجه، ترویج و رونق استفاده از این رویکرد، مستلزم سیاست‌گذاری صحیح است. از جمله الزامات این سیاست‌گذاری می‌توان به تصمیم‌گیری صحیح برای اجرا و استفاده از BYOD، اطمینان از زیرساخت‌های فنی قوی برای اجرای BYOD، وجود پروتکل‌های امنیتی اطلاعات و حمایت از کارکنان و حفظ انگیزه آن‌ها در استفاده بهینه از BYOD اشاره نمود. از طریق سیاست‌گذاری درست BYOD و اجرای دقیق آن‌ها، می‌توان چالش‌های BYOD را کنترل نمود و از مزایای آن در شرایط همه‌گیری به خوبی بهره‌مند شد. استفاده از رویکرد BYOD علاوه بر این که منجر به کاهش مرگ و ابتلا به بیماری کرونا به خصوص در افراد شاغل خواهد شد، می‌تواند به صرفه‌جویی در هزینه‌های سازمان‌ها نیز کمک کند و حتی در دوران پساکرونا نیز به کار گرفته شود.

تضاد منافع

در انجام پژوهش حاضر، نویسندگان هیچ‌گونه تضاد منافعی نداشته‌اند.

References

1. Lazzarotti JJ, Gavejian JC. Work-From-Home Checklist during the Coronavirus Pandemic [Online]. [cited 2020 Mar 16]; Available from: URL: https://www.workplaceprivacyreport.com/2020/03/articles/data-security/work-from-home-checklist-during-the-coronavirus-pandemic/
2. Boda R. Coronavirus: BYOD, working remotely and ensuring information security [Online]. [cited 2020 Mar 19]; Available from: URL: https://www.lexology.com/library/detail.aspx?g=988ab7a1-647e-414c-87a2-3c8ca186c157
3. Stone King. Coronavirus (COVID-19) Data Protection - The keys to securing agile or home working [Onlie]. [cited 2020 Mar 16]; Available from: URL: https://www.stoneking.co.uk/literature/e-bulletins/coronavirus-covid-19-data-protection-keys-securing-agile-or-home-working
4. Zhang Y. COVID-19: Data protection obligations and cyber security advice for organisations [Online]. [cited 2020 Apr 9]; Available from: URL: https://www.burges-salmon.com/news-and-insight/legal-updates/covid-19/covid19-data-protection-obligations-and-cyber-security-advice-for-organisations/
5. European Union Agency for Cybersecurity. Tips for cybersecurity when working from home [Online]. [cited 2020 Mar 24]; Available from: URL: https://www.enisa.europa.eu/tips-for-cybersecurity-when-working-from-home
6. ARXAN. Best Practices for Employee BYOD Training [Online]. [cited 2013 Aug 28]; Available from: URL: https://www.arxan.com/arxan-blog/best-practices-for-employee-byod-training

Health Information Management

Published by ***Vesnu Publications***

Vol 17/ No 2/ June & July 2020

DOI: 10.22122/him.v17i2.4121

Policymaking for Applying the Approach of Bring Your Own Device in COVID-19 Pandemic: A Perspective

Maryam Jahanbakhsh[1], Mostafa Amini-Rarani[2], Shahram Tahmasebian[3], Masoumeh Shahbazi[4]

Commentary

Abstract

By beginning of the year 2020, COVID-19 has spread all over the world. The virus has caused numerous social, medical, and political challenges. One of the major challenges faced by countries to control the outbreak of the virus was the stability of economic and social activities and the simultaneous fulfilling of work during quarantine. Under such circumstances, telework is employed as one of the important policies control the virus. Moreover, many employees have tendency for remote working or teleworking. In such a situation, the importance of applying the Bring Your Own Device (BYOD) approach to fulfill job duties seems obvious. To enjoy the benefits of BYOD, organizations need the right policy for applying BYOD. This perspective endeavors to shed light on how to apply BYOD policy. From the researchers' point of view, the important facets that could be addressed when applying BYOD can be described like this: policy is appropriate decision-making and implementation, technical infrastructure, continuous communication, staff training, security and privacy protocols, and agreement between staff and organization as well as the use of cloud computing.

Received: 04 Mar., 2020 Accepted: 20 May, 2020 Published: 04 June, 2020

Citation: Jahanbakhsh M, Amini-Rarani M, Tahmasebian S, Shahbazi M. **Policymaking for Applying the Approach of Bring Your Own Device in COVID-19 Pandemic: A Perspective.** Health Inf Manage 2020; 17(2): 87-9.

Article resulted from MSc thesis No. 398799 funded by Isfahan University of Medical Sciences.

1- Assistant Professor, Health Information Management, Health Information Technology Research Center AND Department of Management and Health Information Technology, School of Management and Medical Information Sciences, Isfahan University of Medical Sciences, Isfahan, Iran
2- Assistant Professor, Health Policy, Health Management and Economics Research Center, Isfahan University of Medical Sciences, Isfahan, Iran
3- Assistant Professor, Medical Informatics, Department of Medical Biotechnology, School of Medicine, Shahrekord University of Medical Sciences, Shahrekord, Iran
4- MSc Student, Health Information Technology, Department of Management and Health Information Technology, School of Management and Medical Information Sciences, Isfahan University of Medical Sciences, Isfahan, Iran
Address for correspondence: Masoumeh Shahbazi; MSc Student, Health Information Technology, Department of Management and Health Information Technology, School of Management and Medical Information Sciences, Isfahan University of Medical Sciences, Isfahan, Iran
Email: m.shahbazi995@gmail.com