4 tips for securing the digital workspace

Sr. Security Advisor Murtaza Hafizji discusses security for remote work on B2B Tech Talk.

BYOD (Bring Your Own Device) has uncovered a lot of challenges for organizations—namely, security challenges.

Murtaza Hafizji, a senior advisor at RSA Security, offers up 4 expert tips for securing your digital workspace when employees are operating on their own devices.

Plus, Murtaza and Keri talk about:

- The main motivators for leaders to implement BYOD
- The security risks BYOD poses for organizations and how multi-factor authentication (MFA) can mitigate them
- How RSA has successfully enabled essential workers and accelerated digital transformation journeys around the world

Read Murtaza's article, Protection & Peace of Mind During a Time of Business Disruption. Learn more about Identity Management from RSA.

*"The pandemic has worked as a **catalyst** for organizations to **accelerate their digital transformation** journeys." — Murtaza Hafizji*

Despite the benefits BYOD provides, there are some serious threats that need to be addressed when employees are operating on their personal devices.

BYOD risks:

1. Data leakage
2. Sketchy apps being downloaded
3. Lack of corporate oversight/management
4. Malware infiltration
5. Mixing personal and professional use on the same device

To reduce the chance of these threats materializing, consider the following expert tips on securing a remote workspace.

4 tips for securing a remote workspace:

1. Understand that **strong usernames and passwords are NOT enough**. Once bad actors get a hold of login credentials, they're off to the races. Usernames and passwords cannot be your only line of defense—**you need multi-factor authentication (MFA)**.
2. Take a **risk-based approach to access controls**. With a risk-based MFA system, your employees won't be inconvenienced. The system only asks for additional identification if it detects a **high enough level of risk**.
3. Provide **simple and convenient access**. Again, for risk-based MFA to work, your employees have to be on board. That means your MFA system needs to treat your **employees' experiences** as well as your customers' experiences. **Great UX** makes a world of difference.
4. Use a **single interface solution**. Implementing one interface for MFA will make it more **accessible and convenient** for your employees to stay secure when working on their own devices.

Partners can get more information about RSA security solutions by contacting Michael Kline at michael.kline@ingrammicro.com

To join the discussion, follow us on Twitter @IngramTechSol #B2BTechTalk

Sponsored by Ingram Micro Financial Solutions and Imagine Next

Listen to this episode and more like it by subscribing to B2B Tech Talk on Spotify, Apple Podcasts, or Stitcher. You can also listen on our website.