Blog for MPA Networks

https://www.mpa.com/blog.aspx?p=what-you-dont-know-can-hurt-you-the-dangers-of-shadow-it

What You Don’t Know CAN Hurt You: The Dangers of Shadow IT

Posted September 18, 2015

Last spring, Hillary Clinton received a barrage of criticism after it was revealed that she used a private email server during her tenure as Secretary of State—seemingly at odds with government security protocols, if not federal laws. Clinton would go on to publicly dismiss the controversy, saying she simply preferred the convenience of carrying a single mobile device for her government and personal email accounts.

We’ll leave speculation about Clinton’s IT motives to other forums. But everyone can agree the Hillary email controversy is a perfect example of what is commonly termed **shadow IT**: employees and departments acquiring and using devices, software, or online services to solve a specific business need, without their IT department’s guidance, approval, or even knowledge.

BYOD Gone Bad

Think of shadow IT as the dark side of BYOD, which we discussed last time. With so much intuitive technology available to the consumer market (from mobile gadgets to Cloud-based apps), it’s easy for the not-so-tech-savvy to think they’ve stumbled upon an easier way to get their work done. The only problem is that when IT administrators are left “out of the loop,” unchecked shadow IT can open the door to multiple risks—from improper software licensing to network compatibility issues to an all-out security breach.

Can these vulnerabilities be avoided by simply imposing an arbitrary “no shadow IT” policy? Of course not.

The underlying cause of shadow IT is a rigid IT department which is reluctant to accept change. **When employees are not offered better solutions, they’ll seek out their own.**

Out of the Shadows

Shadow IT can be minimized when the IT team sheds its “watchdog” mentality in favor of a collaborative, win-win relationship with the rest of the company:

- Address employees’ **high-priority IT requests** as soon as possible. Streamline evaluation/procurement processes to remove roadblocks to new solutions.
- Keep an open mind to **out-of-the-box ideas**. Don’t shoot down a suggestion by replying, “We can’t do it that way… because that’s not the way we do it.”
- Regularly share information about **emerging security threats**—and how to avoid them.
- Reinforce the importance of following **data compliance regulations**, where applicable.
- Stay ahead of the game by following the latest **IT trends** and suggesting **cutting-edge solutions**.
- Stress the practicality of **centralized IT operations** as opposed to individuals “doing their own thing.”

Effective two-way communication is the ultimate defense against shadow IT. At MPA Networks, we’ve found that this proactive approach has worked wonders for customers who’ve felt bogged down by an unresponsive IT department. Employees are less inclined to look for outside solutions—and ultimately become more productive—when they feel they’re simply being listened to.