IDC ANALYST CONNECTION

Tom Mainelli
Program Vice President, Devices and Displays

The Role of Physical Security in a BYOD World

January 2015

IDC's ongoing research shows that the trend toward support of the bring-your-own-device (BYOD) phenomenon continues to grow. In a recent IDC survey of United States–based IT buyers, fully one-third said their company had already instituted a formal BYOD policy, and another 19% said they expected to institute a formal policy in the near term. Informal support, meanwhile, is notably higher. BYOD brings with it not only a long list of positive attributes but also a set of daunting security challenges for even the best IT organizations.

The following questions were posed by Kensington to Tom Mainelli, program vice president for IDC's Devices and Displays research, on behalf of Kensington's customers.

Q. How has the proliferation of BYOD made the IT organization's job of securing hardware and data more difficult?

A. The job of an IT organization used to be pretty straightforward when it came to the endpoint: Procure, image, deploy, and manage a company's fleet of PCs. Some were desktops, and some were notebooks, but in the end, most ran Windows, and they were all pretty similar. Security is never easy, but with such a homogeneous set of devices, it was fairly straightforward and predictable.

Now, in any given organization, IT is being asked to not only manage and secure a wider range of notebooks and desktops but also wrangle phones and tablets running a wide range of operating systems. The familiarity of these devices — the simple fact that they are used for both work and personal purposes — leads to problems because many end users fail to follow even the most simple and straightforward security measures. Nobody questions the need to password-protect company PCs, but because end users are glancing at their tablet hundreds of times per day, many will skip this most rudimentary level of security on that device.

The rise of the BYOD phenomenon, where end users increasingly use their personally purchased devices to conduct work business, has served to more significantly muddy the waters when it comes to separating work data and private data and the security required for both.

Q. What role does physical security play in the overall security strategy in light of BYOD?

A. On the face of it, BYOD seems like a win-win situation for both end users and IT. The employee chooses which device to carry, and IT transfers the recurring cost of purchasing the device to the employee (often offering a partial stipend and/or paying for service). Forward-thinking IT organizations spell out the rules to BYOD participants up front around data security and the risk they assume when using a personal device for work. One of the stipulations is that, in the event a device is stolen, the employee must notify IT so that the organization can take steps to limit

the risk of data being taken from that device. In other words, IT wipes the entire tablet, erasing business emails and work documents as well as family photos and home videos.

This can be devastating to the employee, especially if those personal files aren't backed up. In many workplaces, the desktop or notebook is secured to the desk at all times. Such physical security is a potent first line of defense and, when combined with a simple password lock, is often enough to keep data safe and secure in the vast majority of instances. As mobile devices proliferate, we expect physical security to become equally important in this domain. Preventing a device from being removed from the workplace by securing it physically has the potential to substantially alleviate much of the risk inherent in the rise of mobile device usage.

Q. What are some of the current solutions or processes in place to address BYOD security?

A. For many companies, the low-hanging fruit around secure BYOD amounted to supporting access to a virtual desktop on the mobile device. To access company email, documents, and other data, the end user was forced to essentially access his/her secure desktop (either an actual PC or a secure desktop in the datacenter) via a secure application on his/her mobile device. While this approach meant that no company data resided on the device, it typically led to a less-than-ideal experience as users struggled to navigate a Windows interface on a smaller phone or tablet screen.

Over time, most companies transitioned to a mobile device management (MDM) solution. These services, still widely used today, typically force the end user to abandon a device's native email client, browser, and apps in favor of secure versions created by the MDM provider. This ensures a much higher level of security but often destroys the user experience. Beyond MDM, mobile application management (MAM) focuses on securing a crucial set of business apps and mobile content management (MCM) focuses on the security of business-critical data. Each of these technologies can play a crucial role in BYOD security. But at the end of the day, if you can prevent a device from being stolen in the first place, you're ahead of the curve.

Q. What are some of the best practices for implementing physical security (i.e., what factors should be considered when adding physical security to an organization's overall strategy)?

A. As with any security measure, the weakest link in physical security will always be the user. A highly complex password won't stop anyone if it's scribbled on a Post-it Note stuck to the computer screen, and the world's best physical security won't prevent theft if it's not engaged. The key to adding physical security is to make it as simple and painless to use as possible. If an employee is forced to struggle with a cable, fuss with a lock, and fidget with a key whenever leaving the workspace with notebook or tablet in hand, chances are the employee will find reasons not to utilize it.

Locking a device should be as simple and straightforward as plugging in a USB-based mouse. This is even more important for highly mobile devices such as tablets. Locking solutions need to be small, unobtrusive, and easy to attach and detach with one hand. Above all else, they have to essentially disappear when an employee is using the device. If employees feel that a lock limits their ability to be productive with a device, they won't stop using the device — they'll stop using the lock.

Q. What requirements should drive the search for physical security solutions?

A. Once the ease of use of a solution is verified, a solution provider must prove its mettle in three key areas: an emphasis on ongoing research and development, strong and deep device industry ties, and a history of both design and business stability. The first requirement may seem counterintuitive if you think a lock is just a lock, but from the time the first PCs

were rolled out in businesses until now, a lot has changed, including the physical security we use. IDC expects that pace of change to continue, so it's important to find a partner that will continue to evolve its solutions as the endpoints change.

You also need a provider that works closely with the device industry on design, standards, and compatibility. This close collaboration was a key to the success of physical security on early desktops and laptops, and it becomes even more important as we move to ever-slimmer devices such as ultrabooks and tablets. Finally, it's important to find a provider that has a long history of both design and business stability and stands behind its products. Big or small, once a company commits to a solution, it doesn't want to find out that its current lock is no longer viable or that the solution provider is no longer around to service ongoing needs.

ABOUT THIS ANALYST

Tom Mainelli has covered the technology industry since 1995. He manages IDC's Devices and Displays group, which covers a wide range of hardware categories including PCs, tablets, smartphones, thin clients, monitors, and wearables. In his role as program vice president, he works closely with company representatives, industry contacts, and other IDC analysts to provide in-depth insight and analysis on the always evolving market of endpoint devices and their related services.