> *Virtualization allows IT managers to implement a level of separation of company data from personal information. The problem for IT is delivering applications to a large number of different devices and platforms. Virtualization solves a lot of issues around this challenge.*
>
> *JIM HENRYS, PRINCIPAL STRATEGIST, INTEL CORPORATION*

Knowing both the setting and the usage scenario helps clarify your security risk. And focusing on business needs helps stabilize your security architecture by insulating it from quickly changing technology fashions.

4. UNDERSTAND THE SOCIAL NETWORK COMMUNITY

In business as in life, authority is based on a web of trust that relies on authentication of identity. In highly secure applications, we authenticate using physical identification: fingerprints, voiceprints, eye scans, and so on. But elsewhere we are content to rely on artifacts—passwords and other secrets, uniforms and badges, seals and certificates, and physical artifacts like keys and cards.

Emerging community technology presents a challenge to traditional authentication strategies, because it permits a person to project his or her identity to smart devices and virtual (software) avatars. Those projections have little accountability and ultimately even their identities must be suspect. (As the saying goes, "on the internet, nobody knows you're a dog.") Yet they can share information with each other and engage in a variety of other collaborative activities. The full implications of this transformation are not yet known, but it is clear they are significant. And social networks are not going away. To the contrary, they are quickly being integrated into workgroups, often with exceptional business benefits.

It is likely that your product will become more social over time, even if you can't currently conceive of moving in that direction. The challenge for security is that the more social your product becomes, the greater is the likelihood of a security breach. Rarely a month goes by without news of significant public exposure of passwords, social security numbers or other identifying information. That kind of lapse used to be exceedingly rare.

With social networking evolving so quickly, specific advice is neither accurate nor useful because it is so quickly out of date. The best advice we can give is more general: you can't ignore social networking—so stay informed, and participate if at all possible.

5. EMPOWER THOSE YOU TRUST

Technology and mobility have empowered us to accomplish, by ourselves, tasks that used to require coordination among several people. For example, on your smartphone today, you can book a business trip to Paris, confirm a meeting there with the CEO of your largest international customer, arrange to take them to dinner, and send them a signed sales proposal that you produced this morning. (With voice recognition, you can do it all in the shower.)

In a world where all that is possible, encumbering any significant business function with too much security process puts the whole business at a competitive disadvantage. In other words, lockdown is not an effective security strategy. Even authentication, if sufficiently complex, can depress usage, and that's the last thing you want happening with your product. In the long run you will profit the most if you can find a way to empower those you trust.

WHAT ABOUT YOUR CUSTOMER'S IT DEPARTMENT?

In choosing your target BYOD platforms, it is important to avoid falling in love with one simply because it promises IT-friendly system management capabilities. That might appeal to your customers' IT departments (and make your sale easier). But if the platform doesn't have widespread consumer adoption, it will have poor business adoption, and your customer won't see the expected benefits. You and your customers will be better off going with widely adopted mobile devices and waiting for their vendors and ecosystems to develop system management capabilities. That is the next frontier for their business models, and they are adapting quickly.

> *Fully 63% of the IT managers surveyed selected data security as their top mobility challenge, while 57% said network security and device manageability were also top concerns.*
>
> *IDG QUICK POLLS MOBILITY, JANUARY 2011*