



Consumer Devices Are Flooding the Enterprise: Run for the Hills? Or Go with the Flow?

A CSO perspective by Dave Martin

Dave is the Chief Security Officer at EMC Corporation and a member of the Security for Business Innovation Council.

Today, it seems everyone has one of the latest smartphones or tablets – and they love it! People get so attached to their favorite gadgets and social applications, they expect to be able to bring them into the office and connect them to the enterprise network – they want to basically merge their personal and business lives together. Who can blame them? Besides being cool and often central to our personal lives, these powerful devices and applications are proving to be business enabling.

As enterprise IT and security professionals, we see the flood of consumer devices approaching and might be tempted to just run for the hills. We're asking ourselves, "If employees start using these devices at work, how do we ensure that these devices don't undo all the work we've put into protecting our sensitive data? If devices are employee-owned, who do users call when they break or have performance issues?" In the past, under a more traditional, rigid security model, we just wouldn't allow the use of personal mobile devices. Period. But times have changed. Today's security teams have to shift their thinking and weigh the business benefits against the risks. It's all about balancing the need for best practice controls against real and tangible business benefits.

The [latest report](#) of the Security for Business Innovation Council, "The Rise of User-driven IT: Recalibrating Information Security for Choice Computing," offers a roadmap for how information security teams can start building out a strategy to enable things like "Bring Your Own Device" programs. If you want to stay ahead of this curve, take a look at this report. It collates the advice of 12 security executives at some of the world's largest companies, with direct quotes on how to tackle this.

One of the things my security team at EMC is monitoring closely is the evolution of virtualization technologies. Newer technologies like virtual desktop infrastructure (VDI) are making it much more feasible to allow employees to use one device for both their personal and working lives while still protecting enterprise data as it stays within the protection of the data center. Through a virtual desktop client, a user can use their personal device to access a virtualized version of their corporate desktop – which works most of the time so long as the host device remains connected, but it doesn't work if the user gets on a plane or in an elevator. Other solutions solve this problem by allowing the virtual image to be mirrored to an encrypted and tightly controlled "container" on the remote device. This brings together the user benefits of choice computing with the supportability and security of a standard corporate image. We're still a couple of years from having enough compute, battery and storage for this kind of container-based solution on smartphones and for now VDI on smartphones will be an online experience. But over the next few years, we expect both hardware and virtualization software technologies to evolve and provide more viable solutions.

End-user awareness will also have to evolve as more consumer devices are allowed in the enterprise. If we allow employees to use their own computers or use personal smartphones for work, the users must have more accountability for their own devices. The education program and support processes we set up must ensure that end-users completely understand their responsibilities.



The Security Division of EMC





From security's standpoint, we need to understand the next generation end-user experience: What is it going to look like? How will we secure it without breaking the benefits of the device? People are going to want access to everything from anywhere using anything. In the course of one day, the end-user will access data over wireless one minute, broadband the next, and LAN the next. How do we keep them plugged in, maintaining states and connectivity without needing them to start some software to reconnect and constantly prompting them to re-authenticate?

Within my security organization, we'd always had leads focused on infrastructure, data security and application security; but a while back, I recognized that in this new "user-driven IT" world, we also needed a specific focus on the end-user. I added an end-user experience architecture lead, who is a key team member in the cross functional team that is joining forces across IT to help EMC transition to enable more choice and mobility in computing.

This position has evolved from having responsibilities for virus and web filtering. Now we're trying to bring these together in a suite of services that also includes the mobility aspects, the user-facing authentication pieces, and VDI – basically everything that touches the user. The goal is to understand what a secure computing experience is going to look like for users in the coming years – whether they are on a mobile phone, tablet or laptop; on the network, their home PC or a coffee shop kiosk.

To match current challenges, most security organizations today are undergoing a cultural shift. Security professionals are increasingly becoming consultants to the business; and focusing on questions like, "How can user-driven IT provide real competitive advantage? How can it positively impact the bottom-line? And what can security do to make it happen while still protecting the business? It's time to innovate our protection strategies and partner with the business to drive value OR get run over by the wave of technology then find another line of work....



Dave Martin, Chief Security Officer, EMC Corporation

Dave is responsible for managing EMC's industry-leading Global Security Organization (GSO) focused on protecting the company's multibillion dollar assets and revenue. Previously, he led EMC's Office of Information Security, responsible for implementing and operating the security controls used to protect the global digital enterprise. Prior to joining EMC in 2004 Dave built and led security consulting organizations focused on critical infrastructure, technology, banking and healthcare verticals. He holds a B.S. in Manufacturing Systems Engineering from the University of Hertfordshire in the U.K. Dave is also a member of the Security for Business Innovation Council.



The Security Division of EMC

www.rsa.com

©2010 EMC Corporation. All Rights Reserved.
EMC, RSA, RSA Security and the RSA logo are either registered trademarks or trademarks of EMC Corporation in the United States and/or other countries. All other products and services mentioned are trademarks of their respective companies.

DM ARTICLE 0710