



From BYOD to BYOA, Phishing, and Botnets

Seth Earley, *Earley & Associates*

Robert Harmon, *Portland State University*

Maria R. Lee, *Shih Chien University*

Sunil Mithas, *University of Maryland*

The consumerization of corporate IT systems is a relatively recent development that has hit IT organizations seemingly out of the blue. One day, desktop computers were provisioned for users, and applications were carefully vetted and controlled. The next thing CIOs knew, they were dealing with laptops, smartphones, tablets, and a raft of new tools and technologies that presented significant security, reliability, and IP protection challenges.

Moreover, users have come to expect an information experience on par with that of their personal lives. Google, Facebook, LinkedIn, Twitter, Pinterest, Skype, and Dropbox are examples of applications that have infiltrated the enterprise's IT infrastructure—whether as an extension of personal productivity applications or as new social-engagement platforms for the business side of the organization. Even for organizations whose policies and firewalls have kept external applications out of the internal information landscape, the game has changed. Users have higher expectations about the ease and speed of information access and the user friendliness of systems required for their jobs.

Clearly, new policies must be enacted and new tools deployed to reduce risks and keep up with growing user expectations, but balancing accessibility and security has proven to be a significant challenge.

Redefining Enterprise IT

This issue of *IT Professional* touches on a number of these topics. In “Consumerization in the IT Service Ecosystem,” Enrique Castro-Leon observes that the trend has redefined IT in the enterprise: “Consumerization has brought an inversion of roles where now users are driving technology adoption and change.” The consumerization of IT is, in part, being pushed by a younger, more mobile workforce comprising active users of new technologies and applications. Employees expect to use their personal devices—and applications—at work, which relates to the concept of BYOX—Bring Your Own Device, Cloud, App, and Network. Instead of new technology flowing down from the business to the consumer, as it did with the desktop computer, the flow has reversed. The consumer market often gets new technology before it enters (and is fully leveraged by) the enterprise.

This blending of personal and business technology is having a significant impact on

corporate IT departments, which traditionally have governed, deployed, and controlled the technology that employees use to do their jobs. Consequently, IT departments must decide how to protect their networks and manage technology that they perhaps didn't procure or provision.

Castro-Leon goes on to point out that users and the employee community don't share this concern: they continue to use their devices as they have in the past, and they expect them to work equally well in corporate settings. Indeed, users want their information experience to be seamless, transparent, and portable, just as they do in the rest of their world. Google, Apple, and Facebook—you've spoiled our users forever.

More fundamentally, this drive for BYOD and consumer-focused IT is emblematic of a larger societal trend facilitated by technology. There has been a shift to part-time, transient, and specialized professional workers. Just as a tradesman used to bring his or her tools to the shop floor at the start of the industrial revolution, the independent contractors filling roles in IT shops, as well as other professionals, are now beginning to bring their own laptops and devices.

Castro-Leon thus also explores how our economy has shifted to value networks and highly interrelated trading partners. As organizations provide infrastructure that's in the cloud, and as information systems transmit data across multiple organizations in a value chain, the boundaries of the enterprise shift and become blurry—especially when software is consumed through cloud-based and hosted application providers. Castro-Leon describes the shift from monolithic to componentized applications, then to Web-services-based applications, service networks, and composite applications, which makes apparent the natural evolution of and connection to BYOD and BYOA (Bring Your Own App), especially as we enter the next evolution of the Internet of Things.

Enforcing Security and Privacy

The flip side of the externalization of software applications and functionality lies in the social component. Services architectures facilitate human-to-machine and human-to-human interactions. The latter allows for opportunities

for the attackers to exploit vulnerabilities due to human nature and the complexity of online social networks, as discussed in "Trust and Privacy Exploitation in Online Social Networks," by Kaze Wong, Angus Wont, Alan Yeung, Wei Fan, and Su-Kit Tang.

In addition to discussing issues around complex privacy settings and the inconvenience caused by enforcing security (which reduces sharing among users), the authors observe that

- the strength of your security level is as weak as that of your friend with the lowest level, and
- your data can be inferred even if you don't disclose it.

Furthermore, attackers have another significant opportunity to access user data: "An app that looks like an interesting game might be designed with the primary purpose of collecting your data. When installing such an app,

Online social networks present a tremendous opportunity for attackers to steal information, spread viruses, and wreak havoc on unsuspecting users.

you might have given the 'game' permission (intentionally or unintentionally) to access your profile, albums, and friends list." Indeed, how often do we casually give apps permission to access various information sources and systems on our devices?

From malware to spam, scam, and phishing (the authors site evidence that 70 percent of the spam on Facebook leads to phishing websites), to botnets, identity forgery, and excess permissions from application installation, online social networks present a tremendous opportunity for attackers to steal information, spread viruses, and wreak havoc on unsuspecting users.

In case you think this is just theory, the authors present an experiment that illustrates five attack approaches: malware, phishing, botnet,

identity forgery, and excess permission requests. Although the experiment didn't cause any harm, the approach persuaded 97 percent of users who installed the Facebook app to give the app permission to analyze their newsfeeds. In addition, 27 percent were tricked into a simulated upgrade of a flash plug-in from a fake YouTube site, which was potentially (not actually) malicious software. The excess permissions allowed a social graph containing almost 20,000 users, even though the app was installed by only 276 people (with the added bonus of social network analysis to identify hubs for more effective malware marketing). Because users access their social networks on the same devices that they bring to work, online social networks can easily become a vector for attacks on corporate data and system security breaches.


Increasing yet Controlling Accessibility

This issue also features related Data Analytics and Securing IT departments, both of which emphasize the need for enterprises to raise the bar on usability and information access while simultaneously establishing and monitoring personal device usage, security, and access policies. These goals seem in opposition—on one hand, increasing accessibility of information, and on the other, controlling that accessibility and dissemination. The trick is to use transparent approaches and a light touch, rather than intrusive approaches that will only encourage workarounds, by leveraging hardware monitoring and management technologies to isolate corporate networks from malware and network intrusions.

In addition to policy development, several classes of technology help IT organizations proactively manage mobile device security threats, including virtualization, walled gardens, and limited separation through a variety of mechanisms that allow access of corporate and personal data on the same device. Although these approaches are complex, they provide viable mechanisms for dealing with the inevitable mix of corporate and personal technologies, letting the enterprise reap the productivity benefits offered by BYOD while effectively mitigating risks and threats.

The goal is to give users the information they need, on the devices they use, from wherever they

work. That is the consumerization trend driven by the macro forces of societal and technological shifts.

The world has changed. This new world of IT provides interesting opportunities and challenges for organizations and IT professionals to deliver industrial grade “SAP-reliable” services while keeping them “Google fast” and “Apple simple.”¹ 

Reference

1. H. McIlvaine, “SAP: Apple Simple, Google Fast,” SAP News Center, 9 Nov. 2011; www.news-sap.com/core-innovation-mobile-in-memory-cloud-snabe.

Seth Earley is CEO of Earley & Associates (www.earley.com). He's an expert in knowledge processes and customer experience management strategies. His interests include customer experience design, knowledge management, content management systems and strategy, and taxonomy development. Contact him at seth@earley.com.

Robert R. Harmon is a professor of marketing and service innovation and Cameron Research Fellow at Portland State University. His interests include IT-enabled service innovation, technology marketing, and big data marketing. Contact him at harmonr@pdx.edu.

Maria R. Lee is an associate professor in the Department of Information Technology and Management at Shih Chien University, Taiwan. Her research interests include social media analytics, e-commerce, and knowledge management. Contact her at maria.lee@g2.usc.edu.tw.

Sunil Mithas is a professor at the Robert H. Smith School of Business at the University of Maryland. His research focuses on the strategic management and impact of information technology resources. Contact him at smithas@rhsmith.umd.edu.



Selected CS articles and columns are available for free at <http://ComputingNow.computer.org>.