Executive Series

Security Essentials for CIOs

Enabling Mobility—Their device, your data

It's not easy being today's CIO. As employees bring growing numbers of their own computing devices to work, CIOs are faced with a tough choice. They must either figure out a secure way to allow employees to conduct business on their own devices—no easy job—or they must simply say no.

This trend is hardly an isolated phenomenon. It grows from the dramatic rise of consumer IT. These days, people regard the gadgets they buy—and love—as tools for their entire lives, including work. This creates a risk of "blurring" personal and professional identities, activities, and information. And this risk of blurring raises important issues for CIOs. You must choose and implement policies and technologies that provide for openness while mitigating risk. This involves a host of thorny questions: How should you protect and segment business data from personal data on a single device? How about managing common challenges like device loss and theft? And what happens to the data on the employee's device when they leave the company?

Highlights:

At IBM, we're constantly striving to find the right balance between openness and risk management. We strongly believe that this balance can be achieved. It involves making clear distinctions between "professional" and "personal" contexts, and then educating employees to recognize and respect these different contexts.

Before embarking on a Bring Your Own Device (BYOD) program, every organization must grapple with these questions and arrive at its own answers. At IBM, we're constantly striving to find the right balance between openness and risk management. We believe strongly, however, that this balance can be achieved. It involves making clear distinctions between "professional" and "personal" contexts, and then educating employees to recognize and respect these different contexts.

Working together, we can manage the risks. And as we see it, there's little choice. After all, enormous innovation is occurring in consumer electronics. The new machines are enabling access in unprecedented ways. So it only makes sense that our employees would be there too, exchanging ideas, making connections, learning about new technologies—sharing vital information with each other. If there's a place for their business activities on their favorite devices, they're more likely to stay in touch with colleagues and customers. They must be active and responsible digital citizens in our hyper-connected era. The technologies and platforms they use are laboratories for innovation.

One critical step is to establish clear boundaries between "personal" and "professional" in terms of digital identities, data, and applications— from a policy and technology perspective.

The key is to harvest these benefits while managing risk. And there's no doubt that allowing the use of personal devices, without first implementing appropriate policy and technical controls, is courting danger. For example, Gartner predicts that by 2013, 80 percent of organizations with BYOD policies will see botnet compromises double inside their networks. As mobile devices carry on business from afar, they extend corporate networks way beyond what used to be considered the perimeter. So securing them is paramount. One critical step is to establish clear boundaries between "personal" and "professional" in terms of digital identities, data, and applications—from a policy and technology perspective. Every single member of the organization must understand these boundaries, and why they're so important to the security of the enterprise. This requires a broad educational initiative extending from far-flung contract workers to the CEO.

Based on our own experience, we'd like to share five steps to consider when embarking on a BYOD program. The goal is to make BYOD use feasible by seamlessly securing corporate data and applications on the device while providing a logical separation from personal activities and data. Additionally, employees must not only understand the risks, but also contribute to the solution. This includes everything from registering their own devices to overcoming the embarrassment of losing gadgets—and reporting a loss promptly.

80%

of organizations with BYOD policies will see botnet compromises double inside their networks by 2013.

Source: http://www.sans.org/reading_room/analysts_program/ForeScoutmobile-security.pdf

All of this requires deep and pervasive awareness, a true risk-aware culture. Building one is serious work. But with senior management support, it is do-able. As you'll see below, we've set out some recommendations on how to extend the mission of enterprise security into the mobile world. But success hinges on the cultural element, a work force that shares the vision, understands the risk and accepts responsibility.

Tips for Enabling the Use of Personally-Owned Devices

1. Establish the rules and spread the word

Working with senior leaders across the organization, the CIO working with the CISO (Chief Information Security Officer) should develop and publish a set of guiding principles on how data can be accessed, consumed, and distributed, and which devices are appropriate for business use. Awareness and understanding of the risk, as well as consensus on the best path forward, are essential for senior management. As new technologies enter the enterprise, these guiding principles will govern what's expected of each employee in terms of security policy and corporate governance.

2. Register every device

The company must have a complete inventory of every device that does business with the corporate network or handles corporate data — its hardware, software and the identities associated with it. There can be no exceptions, because exceptions breed uncertainty, which in turn results in risk. Because of this risk, unknown or unregistered devices shouldn't be allowed to enter the corporate network. And in order to benefit from the flexibility of using personal devices for business, employees should register those devices as soon as they begin using them for work.

3. Common tools

During the registration process, equip each device with a management capability. These technologies enable the technical team to manage configuration and security settings, and establish effective data isolation. Additionally, these technologies should include password protection and auto-lock, and remote-wipe in case the device is lost or stolen. Of course, installation of anti-virus is a critical security control as well. You may also want to consider the use of encryption. It's estimated that over 86,000 laptops were lost by roughly 330 organizations over a twelve month period.[1] If a lost or stolen laptop's hard disk is encrypted, all the data has protection from theft and unauthorized access.

4. Watch Wi-Fi

While Wi-Fi networks seem to be everywhere, not all public ones can be trusted. Educate employees to be careful about using public Wi-Fi networks and not to send sensitive data over networks that are not secure. Encourage them to turn off Bluetooth auto-discovery and scanning and implement VPN software so that employees can connect to corporate data and resources over encrypted channels.

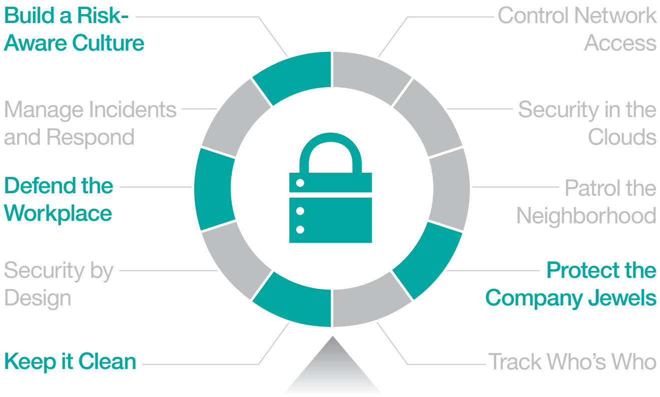
5. Report losses

Employees must understand that if they do business on their personal phone or tablet, it could affect the company's business if they lose it, or even hand it off to a family member. It is important to keep the company's inventory of systems that are used for company business accurate and up to date. What's more, the company should have a specific incident response policy for personally-owned devices as part of its larger policy. Since personally owned devices hold corporate data, they should be managed as carefully as company-owned machines.

Security essentials for CIOs

At IBM, our approach to finding a balance between innovation and the need to control risk involves a set of essential practices. These provide a path to security intelligence in a hyper-connected era.

How do I enable BYOD and mobility?



Balance convenience and responsibility

Join the conversation

To read additional articles, learn more about Security Essentials for CIOs, or share your thoughts with other security leaders join us at **ibm.com/smarter/cai/security**.

About the author

Kristin Lovejoy is Vice President of IT Risk, Office of the CIO, IBM. She can be contacted at **klovejoy@us.ibm.com**.

About IBM Center for Applied Insights

The IBM Center for Applied Insights integrates deep content and analytical expertise to help chart the course to new value for clients. The Center conducts research and builds assets and tools with pragmatic guidance to provoke organizations to action.

[1] "The Billion Dollar Lost Laptop Problem: A Benchmark Study of U.S. Organizations", Ponemon Institute, September 30, 2010 (http://newsroom.intel.com/servlet/JiveServlet/download/1544-8-3132/The_Billion_Dollar_Lost_Laptop_Study.pdf)

IBM Global Services
Route 100
Somers, NY 10589
U.S.A.

Produced in the United States of America
February 2012
All Rights Reserved

References in this publication to IBM products and services do not imply that IBM intends to make them available in all countries in which IBM operates.

♻ Please Recycle