This book explains and then helps readers live with the psycho-techno phenomenon that is bring your own technology (BYOT). Readers will learn how to understand these new end-users and their demands, as well as the strategic and tactical ramifications of these demands. Next, it covers the broad range of technical considerations such as selection, connectivity, training, support, and security. The text includes best practices and case studies of well-known companies, including IBM, Ford, and CarFax."--Provided by publisher.

Includes bibliographical references and index.
ISBN 978-1-4665-6503-6 (hardback)
1. Computer technical support. I. Title.
# Contents

Preface .......................................................................................................................... xv
About the Author........................................................................................................... xvii

## Chapter 1  The BYOD Revolution ................................................................. 1
- What’s in It for the Organization? ................................................................. 2
- So, What Can Go Wrong? ........................................................................... 2
- Mobile Device Management ...................................................................... 3
- Consumerization of IT .................................................................................. 5
- Business as Usual ............................................................................................. 9

## Chapter 2  Making a Financial Case for BYOD ................................. 13
- Supporting BYOD .......................................................................................... 13
- Cost-Benefit Analysis .................................................................................... 14
- Break-Even Analysis ..................................................................................... 15
- Estimating ROI for an IT Project ................................................................. 16
- Earned-Value Management ........................................................................ 20
- Rapid Economic Justification ..................................................................... 21
- Value Measuring Justification Methodology ............................................. 22
  - Step 1: Develop a Decision Framework .................................................... 22
  - Task 1—Identify and Define Value Structure ........................................ 24
  - Task 2—Identify and Define Risk Structure .......................................... 25
  - Task 3—Identify and Define Cost Structure ....................................... 27
  - Task 4—Begin Documentation ................................................................ 27
  - Step 2: Alternative Analysis—Estimate Value, Costs, and Risk ............. 28
  - Task 1—Identify and Define Alternatives ............................................ 31
  - Task 2—Estimate Value and Cost .......................................................... 31
  - Task 3—Conduct Risk Analysis ............................................................. 32
  - Task 4—Ongoing Documentation ............................................................ 32
  - Step 3: Pull Together the Information .................................................... 33
  - Task 1—Aggregate the Cost Estimate .................................................... 34
  - Task 2—Calculate the Return on Investment ....................................... 34
  - Task 3—Calculate the Value Score ......................................................... 35

Bring Your Own Devices (BYOD)Survival Guide
Jessica Keyes
International Standard Book Number-13: 978-1-4665-6503-6 (Hardback)
© 2013 by Taylor & Francis Group, LLC
Contents

Task 4—Calculate the Risk Scores ..............................................35
Task 5—Compare Value, Cost, and Risk ..................................36
Step 4: Communicate and Document ......................................36
Task 1—Communicate Value to Customers and Stakeholders .................................................................37
Task 2—Prepare Budget Justification Documents .............38
Task 3—Satisfy Ad Hoc Reporting Requirements .............38
Task 4—Use Lessons Learned to Improve Processes ..................38
Uncertainty Analysis ......................................................39
Sensitivity Analysis ..........................................................39
Glossary ..............................................................................41
Reference .............................................................................46

Chapter 3 Integrating BYOD into Performance Measurement and Management Systems ..............................................47

Why Measure? ........................................................................47
Understanding Performance Management .................49
Define Organizational Vision, Mission, and Strategy .................................................................49
Develop Performance Objectives, Measures, and Goals .................................................................49
Give Measures Time to Evolve .............................................50
Attributes of Successful Performance Measurement Systems ...........................................................................51
Developing Benchmarks .........................................................52
Plan ......................................................................................54
Collect ...................................................................................54
Analyze ................................................................................55
Adapt .......................................................................................55
Using Balanced Scorecard to Measure BYOD
Effectiveness ........................................................................58
Representative IT Balanced Scorecard Value Metrics ........69
Keeping Track of What’s Going On ....................................70
Validation and Verification ......................................................75
References .............................................................................76

Bring Your Own Devices (BYOD)Survival Guide
Jessica Keyes
International Standard Book Number-13: 978-1-4665-6503-6 (Hardback)
© 2013 by Taylor & Francis Group, LLC
**Chapter 4**  
Assessment and Mitigation of Risks in a BYOD Environment ................................................................. 77

Initiating the Risk Assessment ............................................................ 78
A Typical Organization's Computer System .............................................. 79
System Architecture .............................................................................. 80
System Operational Authority/Ownership ............................................. 80
Threats to A Typical Organization's Assets ......................................... 81
Current Security Measures ................................................................. 83
COG Contingency Planning ................................................................. 84
Divisional Contingency Planning ........................................................ 85
Protection against Network-Related Threats ........................................ 86
Vulnerabilities Reported by the Risk Assessment Team ......................... 87
Recommendations for Mitigating the Identified Vulnerabilities .............. 89
Summary .......................................................................................... 92
Reference .......................................................................................... 92

**Chapter 5**  
Guidelines for Managing and Securing Mobile Devices in the Enterprise .................................................. 93

Mobile Device Overview .................................................................... 93
High-Level Threats and Vulnerabilities ............................................... 94
Use of Untrusted Mobile Devices and Networks .................................. 96
Use of Applications Created by Unknown Parties ................................. 97
Interaction with Other Systems .......................................................... 98
Use of Untrusted Content .................................................................. 98
Use of Location Services .................................................................... 99
Technologies for Mobile Device Management .................................... 99
Components and Architectures ............................................................ 100
Capabilities ........................................................................................ 101
General Policy .................................................................................... 101
Data Communication and Storage ..................................................... 102
User and Device Authentication ......................................................... 102
Applications ....................................................................................... 102
Security for the Enterprise Mobile Device Solution .........................
Life Cycle .......................................................................................... 103
Initiation ............................................................................................ 104
Development ....................................................................................... 107
Implementation ................................................................................... 108
Operations and Maintenance ........................................ 109
Disposal ........................................................................ 110
Case Study ........................................................................ 110

Chapter 6  Cloud Best Practices ........................................ 113
Selecting a Cloud Service ............................................. 114
CSP and End-User Agreements ..................................... 115
Terms of Service Agreements ....................................... 116
Non-Disclosure Agreements .......................................... 116
Service Level Agreements ........................................... 117
Terms and Definitions .................................................. 117
Measuring SLA Performance ......................................... 117
SLA Enforcement Mechanisms ...................................... 118
CSP, Organization, and Integrator Roles and
Responsibilities ......................................................... 118
Contracting with Integrators ......................................... 119
Clearly Defined Roles and Responsibilities .................. 119
Standards ........................................................................ 120
Security ........................................................................ 120
Continuous Monitoring .............................................. 120
Incident Response ....................................................... 121
Key Escrow .................................................................. 122
Forensics ....................................................................... 122
Audit Logs ...................................................................... 122
Privacy Impact Assessments (PIA) ................................. 123
Data Location ................................................................ 124
Breach Response ........................................................... 124
Reference ....................................................................... 125

Chapter 7  Configuration Management in a BYOD Environment ... 127
CM and Process Improvement ....................................... 128
Measurement and Metrics ........................................... 129
Benefits of BYOD CM ................................................ 130
CM Components ........................................................ 130
Configuration Identification ......................................... 131
Configuration Change Control ..................................... 133
Configuration Status Accounting ................................. 135
Contents

Configuration Auditing .......................................................... 136
Implementing CM in the Organization ........................................... 136
Manage the Risks of CM .......................................................... 137
Configuration Management and Data Management .................. 140
  Document Identification ...................................................... 142
  Data Status Level Management ............................................. 143
  Data and Product Configuration Relationships .......................... 145
  Data Version Control ........................................................... 146
  Digital Data Transmittal ....................................................... 147
  Data Access Control ............................................................ 147
Chapter 8  Content Management, Mobile and Otherwise .......... 149
  Content Management System (CMS) ........................................ 151
  Document Management Systems/Electronic ............................... 152
  Document Management Systems (DMS/EDMS) ......................... 152
  Records Management Systems (RMS) ................................. 154
    Reliability ........................................................................ 155
    Authenticity ..................................................................... 155
    Integrity .......................................................................... 156
    Usability ........................................................................... 156
  What Are the Records Management Risks
    Associated with Websites? .................................................. 156
  Digital Asset Management (DAM) ........................................... 157
  Mobile Device Management and Mobile Content
    Management (MDM/MCM) .................................................. 158
Chapter 9  Integrating BYOD into Resource Management ......... 165
  Data Management Roles ....................................................... 166
    Data Sponsor ..................................................................... 167
    Data Steward .................................................................... 168
    Data Administration ........................................................... 170
    Database Administration ..................................................... 172
    System Administration and System Support ............................ 174
  Data Management Responsibilities ........................................... 175
    Development and Management Requirements ........................ 175
    Identification and Enforcement Standards, Design, and
      Implementation .................................................................... 176

Bring Your Own Devices (BYOD) Survival Guide
Jessica Keyes
International Standard Book Number-13: 978-1-4665-6503-6 (Hardback)
© 2013 by Taylor & Francis Group, LLC
### Contents

Data and Mapping Standards ................................................. 176  
Quality Control, Data Integrity, and Backup/Recovery ............... 176  
Data Sharing ........................................................................ 177  
Change Management and Impact Analysis ............................. 177  
Connectivity ........................................................................ 177  
Input and Update ................................................................... 177  
Security .................................................................................. 177  
Metadata .................................................................................. 178  
Training ................................................................................... 178  
Guidelines ............................................................................... 178  
Guideline 1 ............................................................................ 178  
Guideline 2 ............................................................................ 180  
Guideline 3 ............................................................................ 180  
Guideline 4 ............................................................................ 181  
Guideline 5 ............................................................................ 182  
Guideline 6 ............................................................................ 182  
Guideline 7 ............................................................................ 183  
Guideline 8 ............................................................................ 183  
Guideline 9 ............................................................................ 184  
Guideline 10 ........................................................................... 184  
Guideline 11 ........................................................................... 185  
Guideline 12 ........................................................................... 185  
Guideline 13 ........................................................................... 185  
Guideline 14 ........................................................................... 186  
Guideline 15 ........................................................................... 186  
Guideline 16 ........................................................................... 186  
Guideline 17 ........................................................................... 187  
Glossary of Data Management Terms ..................................... 187

### Chapter 10  BYOD Means Social Networking .......................... 195  
Tools That Provide Networking Capabilities ......................... 195  
Wikis in Action ....................................................................... 200  
Meaning-Based Computing ..................................................... 201  
Semantic Web ......................................................................... 202  
Virtual Worlds ........................................................................ 205  
Knowledge Management Tools ............................................. 206  
Mashups .................................................................................. 209  

Bring Your Own Devices (BYOD) Survival Guide
Jessica Keyes

International Standard Book Number-13: 978-1-4665-6503-6 (Hardback)
© 2013 by Taylor & Francis Group, LLC
Contents

References ........................................................................................................................................ 211

Quick Start 1: Software-Based Authentication ........................................................................ 213
  Procedures/Issues/Policies ........................................................................................................ 213
  Bibliography ............................................................................................................................ 213

Quick Start 2: BYOD: Making It Work for Your Firm ......................................................... 215
  Procedures/Issues/Policies ........................................................................................................ 215
  Bibliography ............................................................................................................................ 216

Quick Start 3: Software Selection from Multiple Packages ................................................. 217
  Procedures/Issues/Policies ........................................................................................................ 217
  Bibliography ............................................................................................................................ 218

Quick Start 4: The Make-Buy Decision .................................................................................. 219
  Procedures/Issues/Policies ........................................................................................................ 219
  Bibliography ................................................................................................................................ 220

Quick Start 5: Balanced Scorecard Metrics .......................................................................... 221

Quick Start 6: Common BYOD Mistakes .............................................................................. 231
  Procedures/Issues/Policies ........................................................................................................ 231
  Bibliography ................................................................................................................................ 232

Quick Start 7: BYOD Corporate Policy ................................................................................ 233
  Procedures/Issues/Policies ........................................................................................................ 233
  Bibliography ................................................................................................................................ 234

Quick Start 8: Mobile Device Management Functionality Guide ...................................... 235
  Procedures/Issues/Policies ........................................................................................................ 235
  Bibliography ................................................................................................................................ 236

Quick Start 9: Legal Issues with BYOD ............................................................................... 237
  Procedures/Issues/Policies ........................................................................................................ 237
  The Fixes: How to Inoculate Your Company against Potential Legal Trouble ..................... 238
  Bibliography ................................................................................................................................ 239

Quick Start 10: Managing Online Content Checklist .............................................................. 241
  Procedures/Issues/Policies ........................................................................................................ 241
  General ........................................................................................................................................ 241
  Content Management Issues ..................................................................................................... 241
  Bibliography ................................................................................................................................ 242

Quick Start 11: Selecting a Content Management System
Checklist........................................................................................................ 243
  Procedures/Issues/Policies ........................................................................ 243
  Before You Start .................................................................................. 243
  Determining Project Goals and Targets .................................................. 243
  Determining and Documenting Business Requirements .......................... 243
  Producing Documentation ....................................................................... 244
  Evaluating and Selecting a CMS ............................................................ 244
  Bibliography ........................................................................................ 244
Quick Start 12: BYOD Lessons Learned ...................................................... 245
  Procedures/Issues/Policies ........................................................................ 245
  Each Unique .......................................................................................... 245
  Survey...Survey...Survey ...................................................................... 245
  Clarity ...................................................................................................... 246
  Each and Every Platform Should Be IT’s BFF ......................................... 246
  The App Store Problem ........................................................................ 246
  Virtualization: Might It Be a Temporary Savior? .................................. 246
  Bibliography ........................................................................................ 247
Quick Start 13: BYOD Risks ........................................................................ 249
  Procedures/Issues/Policies ........................................................................ 249
  Bibliography ........................................................................................ 250
Quick Start 14: Getting Started with BYOD .................................................. 251
  Procedures/Issues/Policies ........................................................................ 251
  Bibliography ........................................................................................ 254
Quick Start 15: BYOD Security Tips ............................................................. 255
  Procedures/Issues/Policies ........................................................................ 255
  Bibliography ........................................................................................ 256
Quick Start 16: Cloud Migration Tips............................................................ 257
  Procedures/Issues/Policies ........................................................................ 257
  Bibliography ........................................................................................ 258
Quick Start 17: Hitching Your Network to BYOD ........................................ 259
  Procedures/Issues/Policies ........................................................................ 259
  Bibliography ........................................................................................ 260
Appendix A: Security Glossary .................................................................. 261
Appendix B: Employee Mobile Device Agreement .......................... 271
Appendix C: Mobile Device Security Checklist .............................. 273
Appendix D: Security Configuration Recommendations for Apple iOS 5 Devices ........................................................................... 275
Appendix E: Traditional IT Metrics Reference .............................. 319
Appendix F: Cloud Procurement Questions ................................. 339
Appendix G: Computer Use Policy ............................................. 347
  Acknowledgment ........................................................................ 348
Appendix H: Benchmarking Data Collection Methods ................. 351
Appendix I: Wireless Device Agreement ..................................... 361
Appendix J: Mobile Device Management Vendors ...................... 365
Appendix K: Best Practices Security Checklist .......................... 367
Index .............................................................................................. 423
Preface

BRING YOUR OWN DEVICES (BYOD) SURVIVAL GUIDE

Where once end-users queued up to ask IT permission to buy a new computer or new version of software, they’re now bypassing IT altogether and buying it on their own. From laptops to smartphones, from iPads to any number of software apps, end-users have tasted their freedom and love it. IT is just never going to be the same. BYOD Survival Guide explains and then helps you live with the psycho-techno phenomenon that is “bring your own devices.”

The roots of BYOD can be traced back to the consumerization of all things tech, where technical wizardry is no longer purely the domain of the geek who works for the IT department. Geeks can now be found all over the organization. Many of them are Millennials, the first generation to grow up with computers from birth. These workers want to make their own technology choices, whether those choices are on the “approved” list or not. Whether the company pays for it or not.

BYOD Survival Guide provides the guidance necessary for living in this brave new world. You’ll first learn how to understand these new end-users and their demands, as well as the strategic and tactical ramifications of these demands. We will then cover the broad range of technical considerations such as financial considerations, selection, connectivity, training, support, security, and integration with the cloud and social networking.

But BYOD cannot be considered apart from the rest of the enterprise. It must be properly integrated into the organization’s IT infrastructure, including its information assets. Thus, we will spend some time in addressing topics such as content and data management, risk assessment, performance measurement and management, and even configuration management.

BYOD Survival Guide also comes with a set of Quick Start guides, which provide tips for such things as assessing costs, cloud integration, and even legal issues. There is also a full set of appendices that include information...
on everything from security settings for Apple iOS devices to a sample employee mobile device agreement.

This book is geared for the small- to medium-size enterprises (SME) that need to integrate BYOD into their environment. Since the typical SME does not have the formalized infrastructure that a larger organization might have, we do spend quite a bit of time going over the basics of typical controlling methodologies and discuss how BYOD fits into the picture. Larger organizations may benefit from this discussion as well.

I would especially like to thank those who assisted me in putting this book together. As always, my editor, John Wyzalek, was instrumental in getting my project approved and providing great encouragement. I would also like to thank Debra Nencel, who assisted in the compilation of the Quick Start guides.
About the Author

Jessica Keyes, PhD, is president of New Art Technologies, Inc., a high-technology and management consultancy and development firm started in New York in 1989.

Keyes has given seminars for such prestigious universities as Carnegie Mellon, Boston University, the University of Illinois, James Madison University, and San Francisco State University. She is a frequent keynote speaker on the topics of competitive strategy and productivity and quality. She is former advisor for DataPro, McGraw-Hill’s computer research arm, as well as a member of the Sprint Business Council. Keyes is also a founding board of director member of the New York Software Industry Association. She completed a two-year term on the Mayor of New York City’s Small Business Advisory Council. She currently facilitates doctoral and other courses for the University of Phoenix and is a member of the Faculty Council for the College of Information Systems & Technology. She has been the editor for WGI’s Handbook of eBusiness and CRC Press’s Systems Development Management and Information Management.

Prior to founding New Art, Keyes was managing director of R&D for the New York Stock Exchange and has been an officer with Swiss Bank Co. and Banker’s Trust, both in New York City. She holds a master of business administration from New York University and a doctorate in management from Northcentral University.

A noted columnist and correspondent with over 200 articles published, Keyes is the author of the following books:

- The Productivity Paradox, McGraw-Hill, 1994
- Technology Trendlines, Van Nostrand Reinhold, 1995
- How to Be a Successful Internet Consultant, McGraw-Hill, 1997
- Datacasting, McGraw-Hill, 1997
About the Author

The Handbook of Technology in Financial Services, Auerbach, 1998
The Handbook of Internet Management, Auerbach, 1999
The Ultimate Internet Sourcebook, Amacom, 2001
How to Be a Successful Internet Consultant, 2nd ed., Amacom, 2002
Software Engineering Handbook, Auerbach, 2002
Real World Configuration Management, Auerbach, 2003
Balanced Scorecard, Auerbach, 2005
Knowledge Management, Business Intelligence, and Content Management: The IT Practitioner’s Guide, Auerbach, 2006
X Internet: The Executable and Extendable Internet, Auerbach, 2007
Marketing IT Products and Services, Auerbach, 2009
Implementing the Project Management Balanced Scorecard, Auerbach, 2010
Social Software Engineering: Development and Collaboration with Social Networking, Auerbach, 2011
Enterprise 2.0: Social Networking Tools to Transform Your Organization, Auerbach, 2012
It’s not a question of if. It’s not even a question of when. It’s a question of, will you be ready? Employees have long been using mobile devices. First came laptops, then PDAs. When smarts were added to those PDAs, employees discovered that they could take their office on the road. BlackBerrys became so ubiquitous that the term crackberry was invented to describe the addictive properties of 24 × 7 connectivity. Then Steve Jobs made the smartphone even smarter.

At first, organizations carefully controlled the use of the mobile devices hanging off the corporate network. But employees soon became tired of lugging around multiple devices, one for personal and one for corporate use. Employees also didn’t much like being forced to use a particular device in a particular configuration. Many started sneaking their personal devices onto their corporate networks. And a trend took off.

Let’s look at some statistics. According to Cisco, three out of five workers say that they no longer need to be in the office to be productive. The same research predicts that knowledge workers will have an average 3.3 devices each by 2014. International Data Corporation (IDC) estimates that by 2015 there will be over 200 million mobile workers in the United States alone. Many of these workers are using smart devices such as the Apple iPhone or Android devices. Astonishingly, it is estimated that there are about 400,000 apps in the Apple App Store and over 200,000 apps in the Android Market—now Google Play. So, is it any wonder that over 70% of organizations have adopted Bring Your Own Devices (BYOD)? Further, Gartner predicts this number to increase to 90% by 2014. Most interestingly, a very high percentage of Gen Y workers think that it’s a right rather than a privilege to use their own devices at work.
WHAT’S IN IT FOR THE ORGANIZATION?

The first thing companies think of is cost. BYOD generally shift some costs to the employee. Since employees are paying for their own devices and connectivity the organization can expect to save somewhere around $80 per month per user. This savings can quickly add up.

Another advantage is that most people tend to acquire the latest and greatest technology. Thus, it can be expected that many employees will always have the most recent models of the device and versions of software that runs on that device. Gone are the problems and costs associated with constant upgrading.

Perhaps the most significant benefit is employee satisfaction. Employees can use what makes them happy. In doing so, they’ll be far more productive than if they are forced to standardize on a particular set of devices and software. Some even suggest that employees will work longer hours because they will be able to interact with their systems, using their tools of choice, at any time of day or night.

SO, WHAT CAN GO WRONG?

With the good usually comes the bad. Security is first and foremost. The number of Wi-Fi hotspots has grown exponentially, exposing more mobile devices to hackers who monitor traffic on open networks. In addition, losing a tiny smartphone is easy to do. McAfee, the security company, says that over 4% of smartphones are lost or stolen each year. Each unsecured stolen or lost phone opens the organization up to the chance of a breach of corporate systems and/or data.

Another major concern is how these mobile devices are actually being used. While corporate-owned devices usually come with an acceptable use policy, it’s not all that straightforward to craft such a policy when the device is owned by the employee. Consider how a smartphone may be used. There is a proliferation of social networks and other websites that might be problematic. How should a BYOD acceptable use policy deal with this, if at all?

Costs might be an issue as well. Even though there is a cost saving to the organization as the employee picks up the bill for the device and the
network, someone still has to man the help desk. There is some evidence that calls to help desks about devices not owned by the organization are three to four times more expensive than the equivalent calls for known technology.

Then, there's the data. Some organizations must deal with regulatory mandates that require very strict security measures. How shall this sort of security be architected when BYOD is the paradigm, or on any smart device? Trust is the underlying principle behind enterprise security. Which users to trust and when to trust them should be considered when the organization's security policy is being crafted. What to do about that high-level employee who is given access to proprietary financial data but somehow disables encryption?

Legal experts have weighed in on the subject and found that organizations might be vulnerable in several areas. BYOD necessarily blurs the line between work and play. This creates performance management challenges when trying to regulate on-the-job conduct. There is also a possibility of liability for disability discrimination if the employer finds out, for example, that the employee has downloaded an app for diabetes management and the employee is at some point terminated. Other legal concerns include harassment (e.g., untoward comments), overtime liability (e.g., unrecorded overtime), minimum wage problems (i.e., smartphone users often work long hours), privacy concerns (e.g., what can the employer delete), and workplace safety (e.g., texting-while-driving accidents).

**MOBILE DEVICE MANAGEMENT**

When personal computers became commonplace, organizations realized that they needed to somehow keep track of all of these assets. Thus, asset management was born. Essentially, asset management was a passive systematic process of operating, maintaining, upgrading, and disposing of assets cost-effectively.

With the advent of mobile, asset management needed a shot of adrenalin. This adrenalin is in the form of Mobile Device Management (MDM) systems. MDM secures, monitors, manages, and supports mobile devices deployed across mobile operators, service providers, and enterprises. MDM functionality typically includes over-the-air distribution
of applications, data and configuration settings for all types of mobile devices, including mobile phones, smartphones, tablet computers, mobile computers, and mobile printers. This applies to both company-owned and employee-owned (BYOD) devices.

MDM gives IT the ability to control some aspects of device usage. For example, it can be determined if a jailbroken device is being used. Jailbreaking from the Apple perspective is the process of removing the limitations imposed by the company on devices running the iOS operating system. Jailbreaking allows iOS users to gain root access to the operating system, allowing them to download additional applications, extensions, and themes that are unavailable through the official Apple App Store. MDM also enables IT to forbid devices that aren’t using PINs (personal identification numbers), if this is part of the security policy. MDM permits IT to disable remote e-mail, disconnect users from accessing the network, and even remotely wipe the device. A more complete list of functionality is listed in Table 1.1.

We’ll cover MDM as it relates to mobile content management (MCM) in the chapter on content management.

<table>
<thead>
<tr>
<th>TABLE 1.1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Typical MDM Functionality</td>
</tr>
<tr>
<td><strong>Mobile Device Management Functionality</strong></td>
</tr>
<tr>
<td>FOTA—Firmware over the air updates</td>
</tr>
<tr>
<td>Diagnostics</td>
</tr>
<tr>
<td>Remote Configuration and Provisioning</td>
</tr>
<tr>
<td>Security</td>
</tr>
<tr>
<td>Backup/Restore</td>
</tr>
<tr>
<td>Network Usage and Support</td>
</tr>
<tr>
<td>Server Deployment</td>
</tr>
<tr>
<td>Mobile Asset Tracking and Management</td>
</tr>
<tr>
<td>Remote Lock and Wipe</td>
</tr>
<tr>
<td>Device Provisioning</td>
</tr>
<tr>
<td>Software Installation</td>
</tr>
<tr>
<td>Troubleshooting and Diagnostic Tools</td>
</tr>
<tr>
<td>Policy Application</td>
</tr>
<tr>
<td>Logging and Reporting</td>
</tr>
<tr>
<td>Remote Control and Administration</td>
</tr>
<tr>
<td>GPS Tracking and “Breadcrumb” Mapping (last known location)</td>
</tr>
</tbody>
</table>

Bring Your Own Devices (BYOD) Survival Guide
Jessica Keyes

International Standard Book Number-13: 978-1-4665-6503-6 (Hardback)
© 2013 by Taylor & Francis Group, LLC
CONSUMERIZATION OF IT

Devices are just the leading edge of this revolution. The consumerization of IT, sometimes known as CoIT, also includes, among other technologies, open source software (think Google’s Chrome browser) and cloud storage.

Apple, Google, and even Amazon have cloud offerings. The cloud provides the user with the ability to create, add, delete, and even share information not stored on corporate servers. The cloud is not really all that new. Back in the ancient days of computing, it was referred to as time sharing. However, this was pre-Internet and before there were the security concerns associated with the cloud you hear about today.

In the summer of 2012 these security problems became all too obvious as the press covered in depth the case of some hackers who used what is termed simple trickery to hack a prominent technology journalist’s Amazon, Apple, Google, and Twitter accounts. Security analysts claim that these Internet-delivered services are not doing enough to properly authenticate users. These services require varying amounts of information to open and then access online accounts. Some ask for only a tiny amount of information to make changes. Mat Honan, the Wired journalist targeted, detailed how hackers tricked an Amazon rep into revealing the last four digits of his credit card number. They then used this information to persuade Apple to reset Honan’s Apple ID password, which enabled the hackers to wipe Honan’s iPhone, iPad, and MacBook, destroying all files in the process. A simple solution for this, one which most web services will not offer any time soon due to the inconvenience factor, is multifactor authentication. For example, if I want to change the password on my bank account, my bank will text me a one-time pin that I use to login. Not 100% secure, but far better than what many mobile cloud users are offered.

Aside from authentication, those assessing the use of cloud services for mobile users should closely question cloud services vendors about encryption of information. Questions companies would want answered include which encryption code is being used and information about device hardening methods. Some time ago the Cloud Security Alliance (https://cloudsecurityalliance.org/) created the Security, Trust, and Assurance Registry (STAR), the goal of which is to index the security features of cloud services vendors using a 170-point questionnaire. It’s been a bit slow to catch on, but you can see the completed entries for Amazon, some Microsoft offerings, and Box.com, among others. If your prospective cloud
services vendors are not on this list, then I suggest finding out why. You might also want to download the questionnaire yourself and require these vendors to respond to the points listed.

Still, there is a lot of value in moving to the cloud although cloud computing means different things to different people. In general terms, cloud computing is a convenient, on-demand model for network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. The cloud element of cloud-computing derives from a metaphor used for the Internet, from the way it is often depicted in computer network diagrams. Conceptually it refers to a model of scalable, real-time, Internet-based information technology services and resources, satisfying the computing needs of users, without the users incurring the costs of maintaining the underlying infrastructure. Examples involve providing common business applications online, which are accessed from a web browser, with software and data stored on the “cloud” provider’s servers, as shown in Table 1.2.

The list of cloud computing solutions and service providers continues to grow daily. The sample in Table 1.3 is illustrative and does not imply an endorsement.

Among internal sourcing approaches, the most relevant are the following:

- **Own**—Where the organization that uses the resource also owns or directly controls it. The resource may be totally insourced or totally outsourced, but the organization is its exclusive user.
- **Share**—Where several organizations share the resource, through joint governance arrangements and with one organization being

**TABLE 1.2**

<table>
<thead>
<tr>
<th>Essential Characteristics</th>
<th>Delivery Models</th>
<th>Deployment Models</th>
</tr>
</thead>
<tbody>
<tr>
<td>On-demand Self-service</td>
<td>Software as a Service (SaaS)</td>
<td>Private Cloud</td>
</tr>
<tr>
<td>Broad Network Access</td>
<td>Platform as a Service (PaaS)</td>
<td>Community Cloud</td>
</tr>
<tr>
<td>Resource Pooling</td>
<td>Infrastructure as a Service (IaaS)</td>
<td>Public Cloud</td>
</tr>
<tr>
<td>Rapid Elasticity</td>
<td></td>
<td>Hybrid Cloud</td>
</tr>
<tr>
<td>Measured Service</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

© 2013 by Taylor & Francis Group, LLC
TABLE 1.3

Sample Cloud Offerings

<table>
<thead>
<tr>
<th>Software as a Service (SaaS)</th>
<th>Platform as a Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>Google Apps</td>
<td>Oracle On Demand Apps</td>
</tr>
<tr>
<td>Zoho Office</td>
<td>NetSuite ERP</td>
</tr>
<tr>
<td>Workday</td>
<td>Salesforce.com SFA</td>
</tr>
<tr>
<td>Microsoft Office Live</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>External IaaS</th>
<th>Internal IaaS</th>
</tr>
</thead>
<tbody>
<tr>
<td>HP/EDS (TBD)</td>
<td>Joyent</td>
</tr>
<tr>
<td>IBM Blue Cloud</td>
<td>Rackspace</td>
</tr>
<tr>
<td>Sun Grid</td>
<td>Jamcracker</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Utility Systems Management Tools+</th>
<th>Utility Application Development</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMWare</td>
<td>Xen</td>
</tr>
<tr>
<td>IBM Tivoli</td>
<td>Zuora</td>
</tr>
<tr>
<td>Cassatt</td>
<td>Aria Systems</td>
</tr>
<tr>
<td>Parallels</td>
<td>eVapt</td>
</tr>
</tbody>
</table>

responsible for either owning the resources or sourcing them as deemed fit.

- **Centralize**—Similar to the above, but without the joint governance component. That is, organizations are simply clients of whoever provides access to the resource.

- **Commoditizing**—Where the resource or the way to access it or both is completely commoditized, and it is managed outside the organization’s boundaries without any control of where it is located.

Perhaps one of the most interesting cloud developments is the possibility for IT to provide cloud-based Windows desktop services, with shared resources. This is known as Desktop as a Service or DaaS or hosted virtual desktop (HVD), which works similarly to the client/server model with the server and services being in the cloud, as shown in Figure 1.1. Whether that BYOD user is lugging along his aging Windows XP laptop or a smart new iPhone, HVD enables that user to provide standard office functions.
or application specific functionality. Quite a few vendors have jumped into this marketplace, such as Applications2U, Desktone, dinCloud, ICC Global Hosting, and Nivio, with a May 2012 test by networkworld.com finding that dinCloud was the best of the lot in terms of client options, management, compatibility, and speed.

One of the biggest benefits of cloud infrastructures such as Amazon’s is the ability to store almost unlimited data without having to resort to purchasing new and more expensive servers. This has enabled organizations to amass what is known as big data, traditionally defined as exceeding the ability of commonly used software tools to capture, manage, and process the data within a tolerable elapsed time. It is now easier and cheaper to aggregate data from governmental, academic, in-house, and other sources. It’s data warehousing and mining on steroids.

With big data comes the need to manipulate it. Apache’s Hadoop (http://hadoop.apache.org/) is a framework that allows for the distributed processing of large data sets across clusters of computers using a simple programming model. It is designed to scale up from single servers to thousands of machines, each offering local computation and storage. MapR (http://www.mapr.com/) provides a commercial version of the open source Hadoop. The company provides some insight into how Hadoop can be used:
1. Customer insights—Large financial service providers have adopted Hadoop to improve customer profile analysis to help determine eligibility for equity capital, insurance, mortgage, or credit.

2. Fraud detection and analysis—Hadoop provides a scalable method to more easily detect many types of fraud or loss prevention, and perform effective risk management. Hadoop is also being used to develop models that predict future fraud events.

3. Micro targeting—Banks have numerous disparate data systems (e.g., loans, mortgages, investments) that need to be aggregated in order to provide an up-to-date view on customer profitability, consistent CRM, and customized product recommendations and offerings.

4. Risk mitigation—Hadoop is used to analyze potential market trends and understand future possibilities to mitigate the risk of financial positions, total portfolio assets, and capital returns.

5. Web-scale analysis—Hadoop is used to analyze what is being said on the web at large and on social networks in particular. Sentiment can apply to individual companies or products or reflect general customer satisfaction. This has potential to improve marketing to existing customers through better targeting.

6. Trade analysis—Financial service firms use Hadoop to analyze the daily streams of transaction data in conjunction with unstructured news or social media feeds, or to back-test their trading algorithms.

---

**BUSINESS AS USUAL**

Given all the brouhaha over BYOD, one would expect that the world has radically changed for IT. While it is quite true that there are some major management concerns with the control of these devices, one should not forget that it really is business as usual in terms of data coming into the organization, data leaving the organization, and data being transformed in the middle. Toward that end we’re going to spend the rest of our time talking about how to integrate BYOD into the organization.

Before you embark on BYOD you will want to make a financial case for it. Although the big plus of moving to a BYOD model is that employees cover the costs, this is not the only model and variations really do need to be examined. In addition, there are some hidden costs such as training and
support. Thus, performing ROI, cost benefit, and other financial analyses will give you a true cost picture for the organization and the employee.

Once a financial case for BYOD is made, the organization needs to develop its set of guidelines that will govern managing and securing BYOD as well as non-BYOD mobile devices. This includes use of the cloud, as we discussed above. A “free for all” or ad hoc approach to this is a sure recipe for disaster and presents a great deal of risk for the organization. A more detailed examination of assessment and mitigation of risks in a BYOD environment also needs to be performed.

The Capability Maturity Model (CMM) devised by the Software Engineering Institute of Carnegie Mellon (http://www.sei.cmu.edu/cmm/) has been used by a wide variety of organizations to increase the maturity level of their software engineering practices. A mature IT organization is one most able to align itself to meet the business process objectives of the organization.

The CMM model, as shown in Figure 1.2, consists of five levels of maturity that an IT department goes through on its way to becoming completely optimized and productive:

The initial level (level 1) of CMM is characterized by processes that are ad hoc where tools are informally applied. The repeatable level (level 2) of the CMM is characterized by the achievement of a stable process with a repeatable level of statistical control. The defined level (level 3) of CMM is characterized by the achievement of a solid foundation for major and continuing progress. The managed level (level 4) of CMM is characterized by substantial quality improvements and the use of comprehensive process

![FIGURE 1.2](http://www.sei.cmu.edu/cmm/)

The Capability Maturity Model.
measurement. Finally, the managed level (level 5) of CMM provides evidence of major quality and productivity improvements.

Most organizations hover between levels 2 and 4, although all organizations should strive for level 5. To successfully integrate BYOD into the organization really does require an effort toward enhanced quality, controlled processes, and meticulous measurement. From an IT perspective this translates into tweaking standard processes to accommodate mobile usage. These processes include: resource management, which encompasses mobile device management (MDM); content management; configuration management; and performance measurement and management. All of these processes will be discussed later on in this book.