



Making Your Enterprise Mobile-Ready:

An ebook for IT and Business Executives

Accellion ®

Enterprises at the Crossroads

Most enterprises today stand at a crossroads, tentatively exploring new directions and opportunities for mobile business and IT, but not quite ready to change course from trajectories established years ago.

This hesitation—justified in part by the rapid pace of recent technological change—is evident in the day-to-day experience of workers. New technologies such as mobile computing are being “tacked on” to old IT infrastructure. Traditional workflows and operations are preserved with a few cosmetic changes, rather than being thoroughly reimagined and redesigned. Productivity is edging up, but real progress will only become possible when enterprises fully embrace new paradigms, rather than merely accommodating them.

A mobile-first enterprise—an organization whose services and workflows treat worker mobility as a foundational assumption—stands to become dramatically more agile, efficient, and competitive. Recent advances in technology and design now make it possible for enterprises to embark on new directions in mobile IT and operations while taking full advantage of past investments in technologies such as enterprise content management systems and identity systems. The age of the mobile-first enterprise has arrived.

Two technologies that do promise to reshape organizations and deliver strategic advantage are mobile computing and cloud services.



Most enterprises have reached their current standing in the marketplace thanks to considerable investment over the years in a wide variety of technologies—everything from database servers to instant-messaging systems.

Many of the technologies are mature and well understood. Relational databases have been around for decades. Microsoft SharePoint, an Enterprise Content Management (ECM) platform that as of a few years ago had been adopted by roughly 80% of the Fortune 500, was originally launched in 2001. Microsoft Office—still the de facto suite for creating and editing business documents, slide presentations, and spreadsheets—has been around in its Office configuration since 1988. Web technologies are comparatively newer, but are also mature enough to have been considered mature for many years now. JavaScript libraries are evolving, but the technologies that make up Web applications' basic plumbing—Apache servers and MySQL databases and PHP scripts—are as generic as enterprise IT gets.

While technologies continue to evolve, few executive teams are counting on them to reshape organizations or to deliver critical strategic, “oomph,” to profits and organizational agility.

Finding the Rocket Fuel

Two technologies that do promise to reshape organizations and deliver strategic advantage are mobile computing and cloud services.

In a sense, mobile computing and cloud services technologies are part of the same revolution. Mobile devices, such as smartphones would be just hardware curiosities, admirable for miniaturization, if the mobile devices could access only locally stored data. The amazing utility of mobile devices derives from the ability to instantly access all kinds of data and services in the cloud: everything from email threads; to file repositories; to streaming media; to geo-location services. For the first time, employees in any location seem to have access to all needed data.

This, “whenever, wherever,” access to data ought to make employees more productive. Now employees can look things up and make informed decisions on the spot. Employees can also approve or deny operational requests from conference rooms, hotel lobbies, and taxis. As well as collaborate from the office, a crowded restaurant, or a living room. Everything should happen faster, because no one has to return to desks in order for things to happen at all.

At least, that's the theory.

Which applications are workers primarily using on smartphones? The most popular mobile business application avoids the issue of screen resizing entirely:

 **email**



In reality, there are complications and caveats. Data isn't always so easy to access, and when it's easy, it isn't always secure. Complications and caveats are keeping IT departments busy (and in some cases nervous) and preventing enterprises from realizing the full potential of mobile technology.

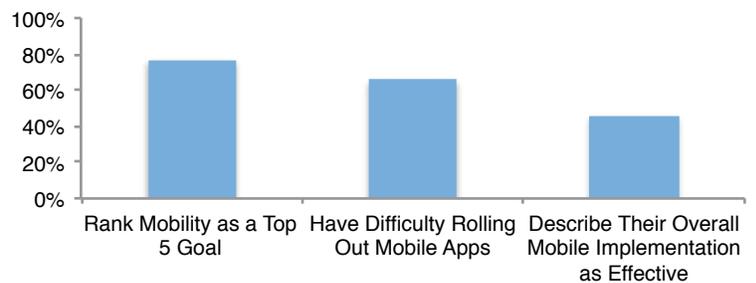
Let's examine several of the complications in turn.

Complication #1: New Devices, Old Infrastructure

Mobile computing doesn't just change where or when employees can access data. It also changes how employees access data. That is, it changes the devices that employees use for everyday work.

Until a decade or so ago, the vast majority of workers used only devices that had been selected and configured by the IT department. Today, thanks to Bring Your Own Device (BYOD) policies that have now been adopted by the majority of enterprises², more workers are selecting

Enterprises have difficulty achieving goals for mobile technology



Source: Accenture

and configuring personal laptops, tablets, and smartphones. As a result, in most enterprises, a bewildering variety of mobile devices now routinely access business data and services from both internal and remote locations.

IT departments, long used to managing one or two desktop systems per employee, now find themselves scrambling to accommodate all kinds of different devices—across a wide number of operating systems. But the complexity doesn't stop there. Not only are the devices different; there are also more of

them. Previously IT might have had to manage BlackBerry devices specially ordered for the sales team and a few executives, but now the average mobile worker carries three different devices, according to a recent survey by iPass.³

That is three devices per employee connected to the local Wi-Fi hotspot, and three devices that need viruses scanned and credentials authorized. Different devices from different vendors support different apps and feature different security strengths and vulnerabilities. Despite the differences and the ongoing introduction of new mobile products from vendors, such as Apple and Samsung; IT is expected to make all devices work and keep all business data safe, while continuing to meet all of IT's other corporate objectives.

When new devices try to access the Web applications and other intranet-based services the organization has put in place over the past decade, challenges arise. Most internal business applications and Web applications were originally designed for desktop systems with average screen sizes of 13 inches. That's about twice as big as the screens of many tablets, and it's three times the screen size of many smartphones.⁴ Applications that are easy-to-use on a desktop system can be difficult or impossible to use on a smartphone.

Mobile Technology: Security Report Card

At the same time that mobile computing is boosting productivity, it's creating new security vulnerabilities that put enterprise content and networks at risk.



- Mobile malware continues to grow in sophistication and number of forms of attack. Between Q1 2013 and Q1 2014, mobile malware forms detected by McAfee Labs grew 167%.
- New forms of malware are taking advantage of vulnerabilities in legitimate applications, making them increasingly difficult to detect.
- Malware-infected devices can spread malware to enterprise networks, where eventually it can reach file servers and other valuable targets. Data breaches that “exfiltrate” data from internal servers can begin with attacks on mobile devices that connect to internal servers.
- Malware can also steal address books and other on-device data, giving hackers valuable information for crafting phishing messages and other forms of attacks.⁵
- When mobile devices are lost or stolen, enterprise data is put at risk, especially when devices are not protected with PINs or passcodes.
- In 2013, 1.4 million smartphones were lost, and 3.1 million were stolen.
- Of the phones that were lost or stolen, only 36% were protected with a PIN, only 29% had data backed up, and only 7% protected data with a strong password or some other device stronger than a PIN. Only 8% featured software that enabled the owner or an administrator to remotely wipe the contents of the device.⁶

The majority of Web applications haven't been rewritten to automatically resize for screen widths. What's legible on the laptop might well be illegible on the smartphone. As employees come to rely more on mobile devices, legacy applications become less useful.

A recent survey found that 82% of mobile users had either never tried to access the intranet on a mobile device or tried and gave up because it proved too difficult. The last decade's infrastructure isn't especially legible on this decade's devices. What applications are workers primarily using on smartphones? The most popular mobile business application avoids the issue of screen resizing entirely: email.

Screen size might seem a minor consideration, but it turns out to be a major obstacle to mobilizing a workforce. Yesterday's applications turn out to be illegible or unusable on the devices that workers are using for a growing share of the work.⁷

Complication #2: Unreachable Content

Speaking of data access, here's another problem. Enterprise Content Management (ECM) platforms like Microsoft SharePoint usually lack connectors for mobile devices. To connect to a file repository like SharePoint or Documentum usually requires connecting through a VPN on



Mobile Productivity? Mixed Results, So Far

In a recent survey of mobile workers, 93% reported that productivity had increased because of mobile technology. Most of the increases were because of traditional applications, such as email, telephony, and remote desktop software, rather than from new mobile apps.⁸

For example, a study of federal workers found that workers with mobile devices put in an extra 9 hours per week, saving the federal government the equivalent of \$28 billion annually. But most of that extra work involved remotely accessing desktop files and apps, and checking email.⁹

When mobile workers try to access other IT services, such as SharePoint or intranets, workers have difficulty. A recent survey by theEMPLOYEEapp found that 82% of mobile workers with corporate Intranets have never tried to access this channel through personal mobile devices, or have a difficult time doing so.¹⁰

Mobile technology makes it easier for remote workers to access email and Web applications. It also makes workers easier to reach reliably by phone. That's good, but it is not enough to give enterprises the return on investment enterprises expected to see from mobile technology. And it leaves past investments in intranets and ECM platforms underutilized.

Enterprises need to do better.

a mobile device. VPNs are notoriously cumbersome on mobile devices, and connections are slow and unstable. Even when VPNs work, mobile users get connected to complex internal directories that have to be navigated on small screens.

To get around difficulties, some IT organizations duplicate ECM content on file servers outside the firewall.

A recent survey¹¹ of 400 IT and security practitioners by the Ponemon Institute found:

- A majority—62%—knew of employees setting up private accounts for public cloud services, such as Dropbox, Google Docs, and Evernote for use in the workplace, even though only 26% of respondents said this practice was permitted.
- 55% of respondents say the risks posed by Bring Your Own Cloud (BYOC) are increasing, and that BYOC affects data security risks overall. What are the risks? According to the study, risks include, “the loss or theft of intellectual property, compliance violations and regulatory actions and loss of control over end user actions.”
- 85% of respondents say BYOC makes it harder to manage access governance and privileged access to sensitive and confidential content.

But duplicating files this way undermines the security policies that made ECM platforms attractive in the first place. It also requires additional expenses in disk farms and file servers and can lead to confusion regarding file versions and edits and a resulting loss of productivity. Ideally, mobile users should be able to connect directly and easily to ECM platforms like SharePoint. In too many enterprises, that's just not possible.

So let's revise our earlier accolades for the mobile revolution. Employees seem to have all the data that is needed, but this is not really the case. So far, all employees really have, are easily accessible data that reads well on tiny screens. As the intranet survey discovered, that turns out to be a fraction of the data that workers need.

Complication #3: From BYOD to BYOC

The need to make files easily accessible leads to another challenge that undermines IT governance and data security.

Understandably, mobile workers want access to all files on all devices. Workers don't want to have to put down smartphones to access data that can be found only on tablets; or put down tablets to access data available only on desktops.

The requirement for instantaneous content access has led to the popularity of file sync and sharing services, which automatically copy and update files and folders across all the devices a user owns. When the IT department fails to provide an easy-to-use solution

Some security threats, such as malware, are technical. Others, such as workers failing to protect devices with PINs or passcodes, are human.



for this critical service, users go shopping for a service. Users can easily find public cloud file sharing services like Dropbox, and will adopt services without necessarily informing the IT department.

In this way, BYOD (Bring Your Own Device) leads to BYOC (Bring Your Own Cloud)—the practices of employees signing up for whatever cloud services employees prefer, without the permission or oversight of the IT department.

Of course, the practice of employees posting business data—including confidential business data and data that is subject to industry regulations, such as HIPAA on poorly secured, unmonitored public cloud file sharing services are a recipe for data leaks, regulatory penalties, and other forms of unpleasantness. Dropbox, for example, once accidentally turned off password protection for all accounts for 4 hours. Users had no way of knowing who had accessed which files during that time.

BYOC is clearly putting enterprise data at risk and is a risky approach for enterprises to endorse. Sensitive data can be anywhere—posted on any random public cloud server, available to whomever. BYOC undermines any IT initiative for data security and data integrity.

A Historical Comparison

To get a sense of how mobile-first applications and workflows might transform the daily lives of workers, consider the evolution of Web technology and early ecommerce sites. In the late 1990's, Web sites were primarily informational, and presented information that had originally been designed for print. When ecommerce sites appeared, the ecommerce sites, too, attempted to replicate print or brick-and-mortar experiences. It wasn't until Web designers stopped trying to imitate print catalogs or brick-and-mortar experiences that Web sites really became fast and easy to navigate.

Business workflows and internal applications need to go through a similar evolution to become much more effective and efficient for mobile workers.

Mobile technology is waiting for a similar revolution. Mobile apps designed from the ground up for mobile devices exist, but many of them are consumer apps. When it comes to enterprise technology, workers



are still forced to connect to an internal network and navigate interfaces designed for desktop computers with 13 to 24-inch screens.

A mobile-first design approach would create apps and workflows from the ground up, recognizing that users will be working on small screens and that tapping and dragging are preferable to typing.



Enterprises must be vigilant about mobile security threats. Employees need to be educated about mobile threats and security best practices. Mobile security solutions need to be deployed with built-in protection, including data encryption and AV scanning.

Diagnosis: Mobility, “Tacked On,” Not Integrated

As risky as BYOC is, however, it highlights an important deficit in most enterprise IT efforts in the area of mobility. Mobile workers are signing up for cloud services to get work done. To work productively with mobile technology, workers need essential services like file sync and sharing.

In too many enterprises, internal IT is not providing file sync and sharing services or are providing file sync and sharing services in an awkward, restrictive way that leads employees to seek workarounds. Part of the problem leading to workarounds is that a lot of legacy enterprise technology is slow and cumbersome on a mobile device.

Consider the basic operation of securely

accessing a file on a SharePoint server. In the desktop era, this was relatively straightforward. The worker would already be on the internal network. He or she would log in through to SharePoint, navigate through the file hierarchy, and find the content needed.

On a smartphone or tablet, this is considerably more difficult. Most ECM platforms like SharePoint lack a mobile interface designed from the ground up for the small screens of smartphones and tablets. And remote access to ECM platforms typically involves a VPN. Entering VPN credentials on a smartphone or tablet is a cumbersome experience. Mobile VPNs are also notoriously slow and unreliable. Once connected to the VPN, the mobile worker has to navigate through the SharePoint interface on a screen that is only a fraction of the screen size imagined by the interface designers.

This example represents the state of mobility in too many enterprises. The IT foundation that enterprises have created over the past few decades still stands. Mobile access has been more or less, “tacked on.” It is possible for mobile devices to access legacy services, but it’s not easy.

Two consequences result. First, workers look for an easier way to get things done, and sign up for BYOC services, such as Dropbox, undermining internal security policies and putting the organization’s regulatory compliance at risk. Second, workers make do with the, “tacked on,” mobile experience, but productivity suffers. Workers put up with slow processes, inscrutable interfaces, and Web forms designed for mouse pointers, not fat fingers.

Workers look for an easier way to get things done, and sign up for BYOC services such as Dropbox, undermining internal security policies and putting the organization’s regulatory compliance at risk.



Complications Add Up: Enterprises Are Falling Short on Mobility Goals

One of the main reasons that enterprises adopt mobility is to increase productivity. It’s true that enterprise productivity is improving, mostly because of longer workdays and extended data access, but for most enterprises mobile productivity breakthroughs and impressive ROI metrics have proved elusive.

Here’s evidence of the shortfall: A recent study by Accenture found that although enterprises were making mobility a top priority, most were having difficulty achieving goals for mobile technology.

What is holding organizations back?

About two-thirds of companies had trouble rolling out new mobile technology. In addition, many reported difficulty in developing and deploying new mobile apps that met employees’ expectations. (The, “tacked on,” mobile experience isn’t meeting employees’ needs.) Enterprises also had difficulty integrating new mobile technologies with existing workflows and infrastructure.¹²



Enterprises should expect to deploy a mix of off-the-shelf and custom mobile apps. Not all business apps will run off the shelf (such as Microsoft Office), some will need customization.

In a nutshell, legacy technology is failing to meet the needs of today's mobile workers.

To date, the increases in productivity that can be ascribed to mobile technology mostly have to do with convenient access to legacy applications. Because workers have smartphones and tablets, it's easier for them to check email at home, and show up in the office ready for action. This kind of benefit is important, but it's still far short of the productivity gains that could be enabled by redesigning workflows and systems to take full advantage of mobile technology.

To realize the full benefits of mobile technology, enterprises need, "mobile-first," solutions for workers—IT solutions designed with smartphones and tablets in mind.

How Should Enterprises Prepare?

In most industries the BYOD trend seems unstoppable.¹³ Enterprises should plan for a BYOD-centered future. Enterprises should expect:

- A fully mobile workforce of tech-savvy employees
- Mission-critical business data stored on mobile devices selected and managed by employees

- Enterprise apps sharing BYOD device resources with consumer apps
- Business data and personal data coexisting on the same device.
- An even faster pace of business, enabled by customers, partners, and competitors also adopting mobile technology and cloud services

Enterprises should expect to deploy a mix of off-the-shelf and custom mobile apps. Not all business apps will run off the shelf (such as Microsoft Office), some will need customization.

On the contrary, enterprises are finding that rolling out approved apps, whether developed internally or purchased "off the shelf," often requires significant internal development work. In a 2012 survey of senior IT executives by IDG Research and SAP, researchers found that over 62% of mobile apps required some kind of in-house programming, whether for light customization or complete implementation.¹⁴

Along with preparing to accommodate more mobile devices and apps, enterprises need to become mobile development experts themselves.

Assessing Enterprise Needs and Goals

Nearly three-quarters of IT executives view mobile technology as transformational or strategic for organizations.¹⁵ To understand mobile transformations in detail, it's worth considering the specific goals and needs of various stakeholders, including managers, workers, and IT.



What Does Your Mobile Workforce Need?

- Secure, easy access to the files and services are needed without VPNs or risky public cloud file sharing services
- Simplicity, not complexity: one interface for all sources of files and content, including Windows File Share, SharePoint, Documentum, and cloud storage platforms like Google Drive, Microsoft OneDrive, and Dropbox
- Context for files: notes and discussions for understanding files and data accessed on a mobile device
- Ability to edit and annotate files securely
- Ability to share files easily with trusted users both inside and outside the organizations
- Task management for managing projects on the go
- A mobile UI that makes it easy to transfer files from folder to another
- AV protection
- Remote wipe capabilities that don't threaten personal data

What Do Most Management Teams Want from a Mobile Workforce?

- Innovation of business processes and offerings
- Increased productivity and efficiency
- No increased risk to security or compliance
- Leveraging existing investments



What Does IT Need to Meet Its Own Goals?

- Centralized control and monitoring
- Data security for all devices and for all business data, whether in transit or at rest
- Flexible, scalable architectures that allow investments to be made precisely where needed
- True integration with legacy systems without cumbersome patches or lengthy development projects

Special Topic: Make Your Internal Operations Mobile

Internal operations such as HR and Legal have yet to fully capitalize on the potential of mobile services.

Legal Department

Take the Legal department, for example. Surveys find that 76% of legal staff are bringing personal mobile devices to work, and 26% of lawyers carry mobile devices with them when traveling. Lawyers should—as it turns out, 40% of law firms expect lawyers to be available for messaging at any time. In addition, lawyers are using mobile devices for reading documents, including legal briefs and reference material.¹⁶ New mobile apps are replacing the law books and binders of notes that lawyers used to have to carry to trial.

In law, data security is essential. Electronic matter that is accidentally disclosed is at risk of losing client-attorney privilege.

Lawyers and legal staff would benefit from secure file storage solutions that support messaging and annotations. Lawyers and legal staff could use micro-blogging-like activity streams to stay on top of fast-breaking news and planning. Centralized access control and monitoring would enable IT administrators and compliance officers to ensure that only authorized users gain access to files.



Human Resources

Like Legal departments, HR departments count on confidentiality. They routinely manage sensitive data, such as healthcare information, contracts and salary information, employee disputes, and details for mergers and acquisitions.

As its name suggests, human resources involves people and lots of face-to-face conversations. Laptops and tablets configured with secure access to secure file lockers enable HR team members to travel from office to office, meeting with managers and workers, while keeping critical data close at hand.

Internal operations, such as HR and Legal have yet to fully capitalize on the potential of mobile services.



Special Topic: Make Your External Operations Mobile

Enterprises have high hopes for mobilizing external operations. The Accenture study mentioned earlier found that for 44% of organizations, opening new sales and marketing channels was a major priority for mobile initiatives. Another 39% were striving to improve field/service and customer service delivery through mobile technology.

How would a mobile-ready enterprise help its marketing, sales, and customer service teams?

By enabling them to collaborate, communicate, and share files quickly and easily on any kind of device. Here are some examples.

Sales

A sales representative has landed at the airport and is driving to meet an important client to close a major deal. While the sales rep has been stuck on a plane, the RFP team at headquarters has been polishing the company's proposal and updating the presentation slides with the latest competitive data. The RFP team posts the files to a secure file sharing service accessible to all authorized users. By annotating the files and providing comments in a threaded message forum, the RFP team can ensure that the sales rep understands the latest changes, even if the changes made were not explained over the phone.

When late-breaking news about a customer endorsement arrives moments before the meeting, sales rep can post a message about the endorsement to the folder being used for the presentation.

The secure file sharing service puts all kind of files at the sales representative's fingertips: everything from Word documents to presentations to videos to CAD/CAM drawings.

Checklist: Is Your Organization Mobile-Ready?

Use the checklist below to assess your organization's mobile-readiness.

STRATEGY

- A published enterprise-wide mobile strategy
- Milestones for measuring the success of mobile initiatives
- Endorsement and monitoring from top executives

SECURITY AND COMPLIANCE

- Security training and best practices for all employees
- An IT-managed app store or whitelist of approved mobile apps
- On-device security for all employees, providing secure containers for business content and AV scanning

DATA ACCESS AND PRODUCTIVITY

- Ability to securely edit, create, and annotate content from a mobile device
- Ability to share content with all authorized recipients, including internal and external users
- Mobile access to business content from any device
- Mobile access to ECM platforms, such as SharePoint, without a VPN

INHOUSE EXPERTISE

- Mobile-savvy development team for developing and customizing mobile apps

WORKFLOW OPTIMIZATION

- Integration of mobile content security with other IT systems, enabling legacy IT services and workflow to be mobilized
- Design focus on, "mobile moments"—situations and locations where on-device capabilities can make a critical difference in actions and results

Contact Accellion to learn how kiteworks can help solve your mobile enterprise challenges, by helping you create customized apps that will improve business processes and enhance productivity, without putting security and compliance of sensitive content at risk.

Endnotes

1. <http://technet.microsoft.com/en-us/magazine/gg981684.aspx>
2. <http://www.zdnet.com/unavoidable-62-percent-of-companies-to-allow-byod-by-years-end-7000010703/>
3. <http://www.ipass.com/blog/mobile-worker-byod-costs-impact-productivity/>
4. Consider an office worker carrying an iPhone 4s smartphone (screen resolution: 1136 x 640) and a Dell Inspiron 15R laptop (screen resolution: 1366 x 768). The screens have similar resolutions, but their different sizes has a major effect on how easy it is to read text and click on the right buttons and menus. The longest side of the iPhone's screen measures about 4 inches; the longest side of the Dell's screen measures about 13.5 inches.
5. <http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q1-2014.pdf>
6. <http://www.consumerreports.org/cro/news/2014/04/smart-phone-thefts-rose-to-3-1-million-last-year/index.htm>
7. For example, 42% of email is now read on mobile devices. <http://www.emailmonday.com/mobile-email-usage-statistics>
8. <http://www.ipass.com/press-releases/mobile-workforce-report-q2/>
9. <http://www.ciainsight.com/it-strategy/mobile-wireless/slideshows/mobile-devices-increase-employees-productivity>
10. <http://www.thecommsapp.com/media-center/press-releases/theemployeeapp-survey-internal-communications-affects-job-satisfaction-and-employee-engagement>
11. <http://whitepaper.techworld.com/cloud-computing/3501984/the-insider-threat-of-bring-your-own-cloud-byoc/>
12. <http://www.accellion.com/blog/accenture-study-finds-enterprises-struggling-to-meet-their-goals-with-mobile-computing>
13. Gartner notes that by 2016, 38% of employees expect to stop providing workers with mobile devices. Workers will be expected to furnish their own. <http://www.gartner.com/newsroom/id/2466615>
14. <http://blogs.sap.com/innovation/files/2012/06/Mobile-in-the-Enterprise-The-Gap-Between-Expectations-and-Expertise-.pdf>
15. <http://blogs.sap.com/innovation/files/2012/06/Mobile-in-the-Enterprise-The-Gap-Between-Expectations-and-Expertise-.pdf>
16. <http://www.accellion.com/sites/default/files/kiteworks-for-teams-Legal.pdf>



About Accellion, Inc.

Accellion, Inc. is the industry leader in providing private cloud solutions for secure access and sharing of enterprise information across devices, enabling employees to work securely wherever. Founded in 1999, Accellion is an award-winning, private company headquartered in Palo Alto, California with offices in North America, APAC, and Europe. The company has evolved from its roots in cloud storage into a leading enterprise security software provider. More than 12 million business users and 2,000 of the world's leading corporations and government agencies, including Procter & Gamble; Indiana University Health; Kaiser Permanente; Lovells; Bridgestone; Harvard University; the Securities and Exchange Commission; and NASA use Accellion solutions to protect confidential information, ensure compliance, increase business productivity, and reduce IT costs.