Mobile applications are changing and will continue to change business operations because of the new practices, opportunities, and risks they present. Businesses can interact with their consumers through mobile apps unlike ever before. They have access to real-time information and a connected platform that is always carried by the person. For example, certain companies can increase their revenue by sending users coupons based on their geographic position relative to a store, retaining payment information for mobile purchases, or notifying people about sales. Mobile applications can also help yield more productive workers and business relationships. Employees and partners can access the company’s app to work and use data away from the office improving operational efficiency, mobility, and connectivity. However despite these advantages, over two-thirds of all firms selling consumer goods did not have mobile strategies in 2011.¹ With strategic plans to integrate and evaluate mobile applications within the IT infrastructure and business processes, companies can access a broader market and cut costs before their competitors. The app can also be monitored and improved by comparing its current functionality to its planned benchmarks and users’ assessments and suggestions.

The “BYOD” (Bring Your Own Device) phenomenon has also emerged as a major business operational change. BYOD is an IT policy where employees are encouraged to access company enterprise systems and data using their own mobile device.² Downloadable mobile applications have allowed businesses to escape stringent IT guidelines. Formerly employees were given specific hardware that could only be used for company functions. Now people in many companies bring their own preferred devices to work. In a 2013 survey, 60% of surveyed

firms allowed for the use personal devices for work while 14% planned to allow it within a year. With the allowance of BYOD, IT typically can cut its hardware and service expenses.

With these new practices and opportunities, new security and support risks have emerged as well. In an Oracle survey of top executives, 53% of the respondents have deep concerns regarding application security and 63% have deep concerns regarding data security. Three of the primary security concerns these executives could have are the confidentiality, data integrity, and availability for mobile apps. Confidentiality is the unauthorized or unwanted exposure of a company’s systems and data. Data integrity is the assurance of the accuracy and consistency of data during its transmission, process and storage. Availability is alluding to the communication channels of the app remaining unaffected and accessible despite disruptions. The business can limit these risks by incorporating mobile application management (MAM), mobile app authorization standards, continual updates, and various other security and functionality processes.

Some employers still use traditional mobile device management (MDM) to handle confidentiality, integrity, and availability risks for BYOD and mobile apps. MDM has the employer infiltrate the entire mobile device to enforce security standards. The company can control a person’s use of their device through disallowing certain functions and apps. MDM gives the company the potential to access personal information. If a worker lost their device or left the company, MDM oftentimes only allows the company to wipe the entire phone,

---

5 Various sources were used that are cited below in the creation of the definitions of confidentiality, data integrity, and availability.
eliminating business and personal data. With such effects, MDM can cause employee dissatisfaction. For a BYOD mobile app strategy to work, the employee’s personal data needs to separate from the company data. To maintain the employer-employee trust, MAM has emerged as the better alternative to MDM. MAM takes an application-centric approach to limit security risks by fortifying company data in its own container away from personal data. MAM does not intrude on privacy or restrict personal application and data usage. It allows the entity to securely govern its data and closely manage or delete company information within the application.

With MAM’s powerful governance capabilities, further data integrity and confidentiality issues can be mitigated. To prevent data from being compromised, mobile applications must communicate in a secure fashion with the home enterprise. By integrating MAM into a company’s IT infrastructure, the company can be alerted to and combat wrongful uses of the applications. An active access management system for MAM and the company’s IT structure can ensure data compliance and protection. Additionally with mobile apps feeding data into the company’s system in real time, data entry can be erroneous and repetitive. Active communication and mobile quality check initiatives through MAM can prevent and detect erroneous and falsified data.

Applications can also mitigate these security risks through authorization methods and encryption. For example, when the person first downloads the app, they could validate the

---

download through their email. Therefore if the application were used to buy a product with credit card information, the owner of the credit card gets an email receipt to confirm the purchase. For inter-firm applications, the app could require a username and passcode every time to open sensitive information. Without these credentials, the mobile application functions and data remains locked and ciphered. These changes seem simple, but they can save the consumer’s and the business’s confidential information from infiltration.

If a mobile app is not loading or is drawing an error, it is unavailable. While security measures defending against infiltration and corruption promotes availability, the application needs to be engineered so it can handle other events. For example, the application should be robust enough to handle a high frequency increase in usage. Specific examples of promoting availability include but are not limited to supporting application functions through cloud computing (a network-based form of application support allowing for on-demand access) and fault tolerant systems (a system that can run while having an error). Ensuring availability constantly involves evaluating the application through attempted hacks, third party reviews, and various stress tests. The application needs to be continually updated resolve these issues.

In conclusion while many businesses are patch-working mobile applications into IT infrastructure, the right architecture is necessary to properly integrate mobile applications into an IT infrastructure. Through proper integration, mobile applications can mitigate security risks and maximize revenue opportunities.

---

Works Cited


<https://blogs.oracle.com/OracleIDM/entry/it_s_time_for_businesses>.


