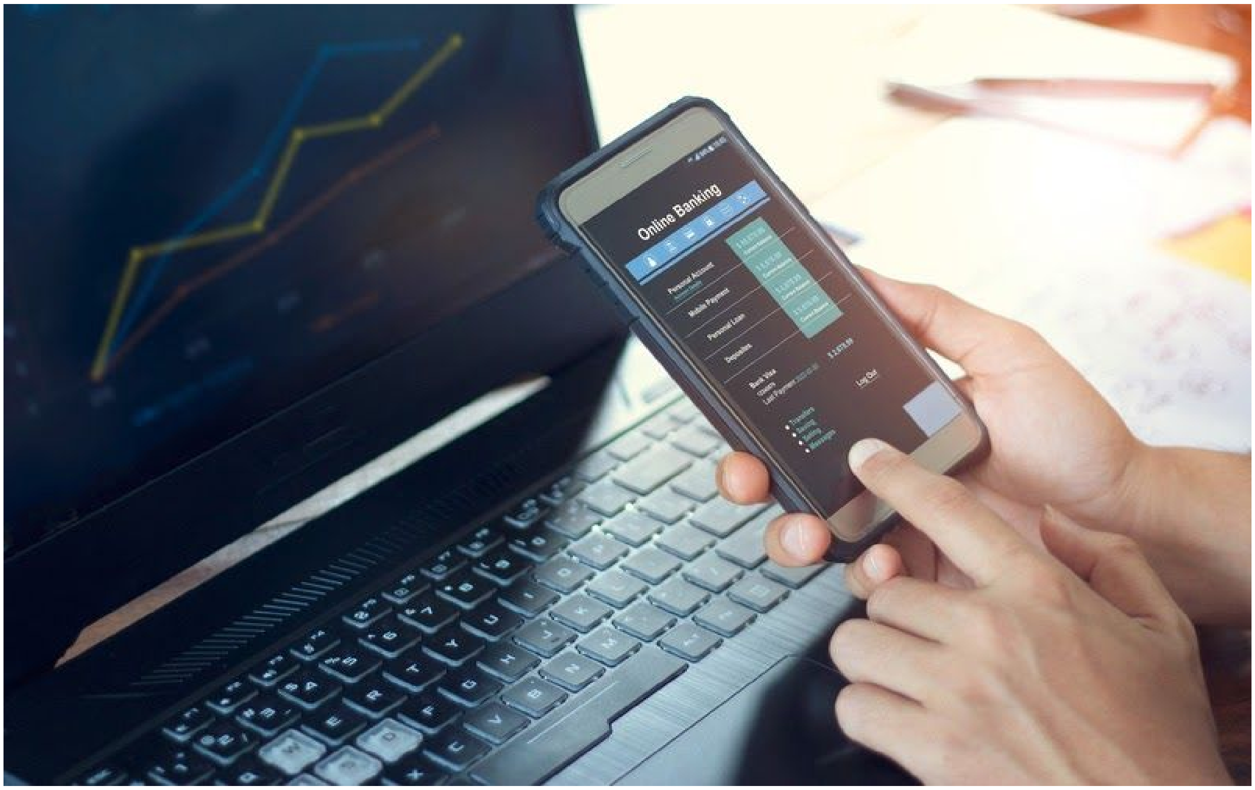
How to Weigh the BYOD Advantages and Disadvantages for Your Bank’s Remote Workforce

by Jenny Kanevsky | Jan 6, 2021 | Financial Institutions | 0 comments



All industries face cybersecurity risks and attack costs. In banking, these concerns can be catastrophic due to their high-value and the nature of the data they secure. In 2019, a hacker breached mega-bank Capital One gaining over 100 million personal data records. Capital One customers suffered, the bank lost credibility and invested significant financial resources in new cybersecurity systems. According to the New York Times, a year later, the bank paid $80 million to settle federal bank regulator claims that it lacked sufficient cybersecurity.

The banking industry is changing due to COVID-19-related remote workforce growth and increased online client traffic. According to Forbes, during the first wave of the COVID-19 pandemic, bank employees’ global mobile device use increased by at least 80%. And, that trend is likely to continue.

Digitization is not new to banks. Even before COVID-19, banks sought efficiency and increased customer satisfaction in modern technology. However, many companies had to accelerate digitization efforts when the pandemic hit, often without comprehensive transformation plans. One of the most significant banking industry changes was the rise in a remote workforce. For CISOs and cybersecurity teams, this created considerable risk and exposure.

According to recent Aite Group research, 94% of attacks on banks originate through employee phishing emails. As more employees use mobile devices to conduct bank business, they put enterprise data and Personally Identifiable Information (PII) at risk. Human behavior is also a concern, and opening an infected email is all too common. Employees worry about the pandemic, and bad actors capitalize on this. In March of 2020 alone, COVID-19-related phishing attacks increased 667% over February, and those numbers have only gone up.

Banks must find strategies to protect and secure their systems and customers. Some banks protect this data by implementing a mobile security solution and supplying company-issued devices or establishing personal device use protocols with a Bring Your Own Device (BYOD) policy.
When building an effective policy, banks should consider the BYOD advantages and disadvantages and how different mobile security solutions impact successful implementation.

Generational Growth to Meet Consumer Needs

For decades, the banking industry has sustained the physical spaces and the on-site transactions they represent. Paper money and checks are less relevant today, and banks are adapting to the paradigm shift. According to a recent DepositAccounts survey, 91% of Americans are banking virtually, including 81% of baby boomers.

The smartphone platform attracts most remote banking customers due to its convenience. Simplified sign-in processes, intuitive interfaces, and real-time information make app-based banking a popular option. According to a JD Power study, in 2020, 30% of banking consumers set up new accounts online or through a mobile app.

Website and mobile platforms improve banking efficiencies. Digital platforms are always open, pandemic or not, twenty-four hours a day. These platforms handle high customer volumes and are precise with transactions and records. They are also relatively inexpensive to maintain, upgrade, and market. These advantages, coupled with their rising consumer popularity, make mobility a strategic investment for banks looking to grow.

How Mobility Meets Banks’ Remote Work Challenges – BYOD Advantages

Mobilization allows banks to meet customer demand and address operational and business objectives. Effective mobility solutions and BYOD policies mean increased remote productivity opportunities and access to a more diverse and competitive talent pool. Employees who don’t need to commute save time and money while employers save on hardware and overhead costs.

BYOD programs save banks on costs associated with company-issued devices and maintenance. Employees typically cover personal device service plan expenses, though some employers contribute to those costs under specific BYOD policies.

BYOD programs empower workers to be more efficient. Employees benefit from a simplified platform, seamlessly moving between work and personal life on the same device, and banks benefit from faster communication and real-time collaboration.

BYOD Security Considerations

While industry indicators show financial institutions benefit from the remote-banking shift, there are security factors to consider. Digital adoption rates are increasing, with the smartphone platform leading the charge. Meeting these customers online is a remote team of banking employees reliant on mobile technology. Deploying resources to meet the demands of a digital office space can be a challenging endeavor.

Mobile devices are vulnerable to attack, break, and are lost or stolen with regularity. Enabling a remote workforce with mobile devices is a strategically necessary step to remain competitive in today’s banking industry. Securing these devices is essential for banks to take advantage of mobile devices’ efficiencies and protect critical consumer and enterprise banking data.

Mobile Device Management: An Imperfect BYOD Solution

Mobile Device Management (MDM) has been the traditional BYOD solution. However, it has drawbacks. While MDM can offer high local security levels, allowing control of the entire device, including the hardware, MDM programs have high upfront, ongoing maintenance, and administration costs.

While company-issued devices are rare today, banks may implement MDM by purchasing devices for their workforce. The initial outlay cost varies considerably based on purchased device quality and workforce size. For MDM allowing personal device use, a common budget-conscious approach, banks must manage, maintain, and update thousands of individual, often out-of-date and unsafe devices.

MDM only protects devices, not data. These limitations force banks to rely heavily on strict, often overreaching BYOD protocols, including complex usage policies, service entanglements, and privacy concerns. Also, MDM tries to confine the BYOD device to banking standards. The attempts come with performance, privacy, and security issues by dragging performance down and forcing IT administrators to completely wipe all business and personal data if a security issue arises.

Banks manage MDM BYOD programs with invasive remote command and control features that allow IT administrators to surveil devices and read and manage device data. These security methods risk personal and business data exposure and create liability and regulatory issues.

MDM BYOD programs depend on employee adoption and adherence, though strict protocols result in employee mistrust, circumvention, or rejection. MDM also requires banks to provide support, service, or, in some cases, personal device replacement. Even if banks implement and maintain a BYOD program with MDM, data protection ultimately depends on employees. This broad risk factor triggers regulatory concerns, which creates more hurdles.

Virtual Mobility Solutions: A Better Way to BYOD

BYOD in banking is the future, and delivering modern banking technology and service while maintaining the highest mobile security level is possible. Banks can reap BYOD benefits while resolving regulatory and security concerns by choosing the right mobile security solution.

Efficient remote productivity and secure data transmission are possible with Hypori Virtual Mobility™. Virtual Mobility BYOD programs thrive without the security, privacy, or cost concerns inherent in MDM solutions.

Hypori® keeps enterprise data on the corporate server and maintains 100% separation between company and personal information. Employees access the bank network through a user-friendly app interface that enables virtual data interaction.

Hypori's next-gen virtual design and military-grade security enable banks to meet GLBA and privacy regulations. Its central administrative hub streamlines IT efficiency, lowering overhead costs in the process. Banks seeking secure, centrally managed, budget-conscious BYOD are ready for Hypori.

Learn more about how Hypori can deliver BYOD to your bank's remote workforce.