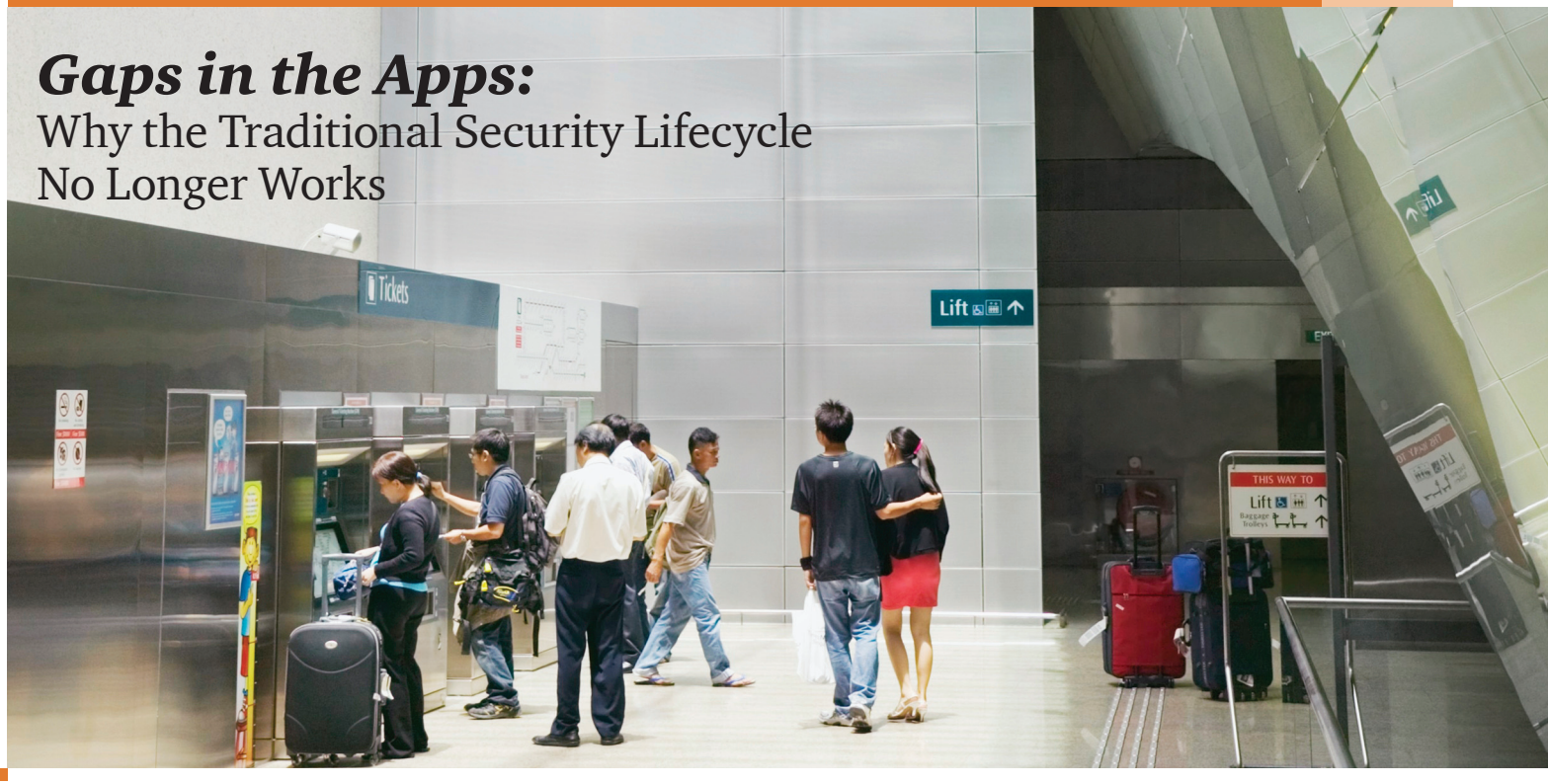
fs viewpoint

www.pwc.com/fsi

April 2012

Gaps in the Apps:
Why the Traditional Security Lifecycle No Longer Works



pwc

Point of view

Banks are at a turning point where it is more likely than ever before that a security incident will cause customers to switch financial institutions.

The rise of mobile payments—and the rapid growth of new non-bank competitors—has provided consumers with an abundance of banking alternatives.

Internet companies such as PayPal and Obopay have been gaining in popularity as convenient, secure channels for executing monetary transactions. At the same time, the telecom industry has ventured into the payments space, enabling users to make payments through text messages and other means. Retail chains, such as Starbucks, have also developed their own mobile apps, which allow users to make payments through barcodes that are displayed on their mobile phones.

Customers are sharing their experiences in real time. Even a minor security incident can become national news in a matter of minutes.

The proliferation of social media has taken word-of-mouth marketing to exponential levels. Customers are using this platform to actively spread the word in real time about their customer service experiences.

Word travels faster than ever before when things go wrong. Customers can publicize security incidents immediately and quickly share steps to others in their network about how to switch institutions.

Customers are sharing their experiences in real time. Even a minor security incident can become national news in a matter of minutes.[1]

The average Facebook user has 130 friends who can find out about a bad banking experience within seconds. On the other hand, well-treated customers are becoming unofficial spokespeople for certain brands.

The disintermediation of banks in consumer payment habits will increase the ease of switching banks.

Today, many consumers have bank accounts linked to several payment sources and destinations, causing significant effort in changing banks. In the near future, mobile banking may allow consumers to disintermediate their checking accounts from these activities, allowing for painless switching of bank accounts.

1 Shayndi Raice, "The Facebook IPO: The Man Behind the Social Network's Marketing," February 2012, www.wsj.com.

The explosion of mobile banking has ignited a race to develop mobile banking applications. In many banks, however, the design and the implementation of sound security measures have failed to keep pace.

The use of mobile banking is dramatically escalating. At the same time, the lack of strong security measures is increasing the likelihood of data breaches—making sensitive customer data a prime target for criminals and exposing financial institutions and their customers to associated risk.

Case in point—in February 2012, a popular mobile payment service disabled one of its offerings after a serious security flaw was discovered. The security issue would have potentially allowed someone to access prepaid card balances stored on a lost phone. Not only was part of the mobile payment service not available to customers for several days as a fix was developed—it also left many customers wondering about the safety of the service and whether they should continue using it.[1]

The transformation of mobile banking…

Before 2010, mobile banking was most often performed via short message service (SMS) or the mobile web. Within the past two years, Apple's iPhone/iPad, Google's Android OS, and RIM's BlackBerry have collectively transformed the ways in which consumers interact with their mobile devices.

Mobile banking is now largely transacted using special client programs called applications, or "apps," which are downloaded to mobiles.

In response to increasing customer demand for service anywhere and anytime, financial institutions are racing to develop mobile banking and payments apps—and sometimes, security policies and standards are not fully considered.[2]

The skyrocketing use of mobile banking apps is putting sensitive customer data—and financial institutions—at risk.

- Current forecasts suggest that **53 million** people will be using mobile banking applications by 2013.[3]
- Several forecasts predict that **50% or more of** US mobile users will be conducting banking transactions from their mobile devices by 2015.[4]
- Consumers are demonstrating an increasing desire to check account balances, pay bills, and transfer funds with their phones.

1 Lance Whitney, "Google Wallet Fixes Prepaid Card Security Bug," February 2012, news.cnet.com.

2 Spence E. Ante, "Banks Rush to Fix Security Flaws in Wireless Apps," November 2010, www.online.wsj.com.

3 TowerGroup, "Customers' Need for Any Time, Anywhere Account Access to Draw over 53 Million Mobile Banking Users by 2013," May 2009, www.towergroup.com.

4 eMarketer, "Mobile Banking Financial Service Firms Looking to Cash In," May 2010, www.emarketer.com.

PwC has seen one institution's mobile innovation pressure other institutions to rush out and develop a similar functionality, circumventing security safeguards in the process.

A good example of innovation in mobile banking is the introduction of remote check deposit technology. This technology enables a consumer to deposit a check by taking a picture with his or her smartphone and uploading the image directly to the bank.

Once a national bank introduced this feature—making the technology available first to iPhone users in 2010 and then to Android users in 2011—other banks were left scrambling to catch up. Leading banks continued to push the innovation curve with the introduction of Person-to-Person QuickPay [SM]. Other banks continue to play catch-up in the mobile app space.

The race to develop innovative mobile banking and payment apps is very real indeed, as underscored in PwC's recent FS Viewpoint:

"The potential value at stake for financial industry participants is up to $20 billion in annual revenue—through both new revenue opportunities and potential loss mitigation. Financial institutions have been cautious entrants into this space, leaving the door wide open for a leader to emerge and gain significant first-mover advantages…The question for most observers remains, 'Who will be the winner in the emerging space?' Traditional players currently have an early lead; however, if they do not keep up with the fast pace of change, tech innovators and collaborators will prevail … Inaction is not an option."[1]

$20B

The amount of potential value at stake in mobile payments[2]

1 PwC, "Dialing up a Storm: How Mobile Payments Will Create the Most Significant Revenue Opportunities of the Decade for Financial Institutions," October 2011, www.pwc.com/fsi.

2 Ibid.

As the impact from identity theft and mobile-application security breaches becomes ever more frightening for consumers, we anticipate that regulators' focus on data protection will intensify in the coming years.

In fact, regulators are already beginning to develop mobile-application guidelines designed to curb harmful trends (such as hacking or malware).[1] However, compliance with regulations alone may not provide sufficient protection against security breaches. Strong security measures are required.

Leading institutions are implementing security measures to protect their financial and reputational well-being against three key risk areas: [2]

Risk areas	Measures being implemented at leading firms
Privacy	• Protecting the customer's sensitive information from exposure to unintended third parties • Preventing identity impersonation from lost or stolen mobile devices or device credentials • Preventing account takeover or identity impersonation from credentials harvested via key loggers or other malware
Fraud	• Preventing money laundering and terrorism financing from the use of compromised accounts • Preventing investment fraud from compromised bank accounts • Preventing "smurfing" (splitting of large financial transactions into smaller transactions) • Preventing the disguise of mobile transaction totals, origins, and destinations
Compliance	• Implementing measures to maintain compliance with multiple laws, including: Anti-Money Laundering Act and Know Your Customers legislation (e.g., USA Patriot Act) • Combating terrorism finance • Undergoing scrutiny by the SEC, Federal Trade Commission (FTC), and Federal Financial Institutions Examination Council (FFIEC) • Monitoring emerging legislation that may impact mobile security, including the Dodd-Frank Consumer Protection Act

1 Verizon RISK Team, "2011 Data Breach Investigation Report," 2011, www.verizonbusiness.com

2 PwC, "Dialing up a Storm: How Mobile Payments Will Create the Most Significant Revenue Opportunities of the Decade for Financial Institutions," October 2011, www.pwc.com/fsi.

When an institution's application development lifecycle lacks sufficient security focus, both the institution and the customers who use its mobile banking apps are vulnerable.

Financial services institutions without an accurate inventory of where personal data for employees and customers is collected, transmitted, and stored[1]
54%

Ethical hacking engagements by PwC that were successful in gaining access to highly sensitive information[2]
90%

Financial services institutions that are following leading practices for mobile application security[3]
25%

In today's open, collaborative, and fast-paced environment, a lack of sufficient focus on security puts institutions and apps users at risk. Unfortunately, the need for speed often trumps the need for data security.

- The *Wall Street Journal* reported that ViaForensics, an innovative digital forensics and security company that focuses on mobile forensics and proactive forensic security, released a publication citing a number of data security flaws in leading banking applications for the iPhone and Android platforms.
- The report also cited mobile-application holes that left users vulnerable to man-in-the-middle and phishing attacks. Phones were found to be storing sensitive information such as banking applications' usernames and passwords; account balances; payment records; answers to security questions; and, in some cases, even bank routing numbers. Some applications were found to be storing this information in plain text on the phone, requiring little smartphone savvy to access the compromised information. The *Wall Street Journal* also reported that a major bank's iPhone application had been saving users' account numbers on the device.[4]
- Eight out of ten CIOs believe that using smartphones in the workplace increases the vulnerability to attack; these CIOs rank data breaches as their top security concern.[5]
- 69% of executives and security practitioners believe that mobile computing represents the greatest threat to information security.[6]

1 PwC, "The Privacy Paradox: The Challenges of Locking Down Data in an Open World," October 2008, www.pwc.com/fsi

2 PwC, "Show Me the Money – Are Cyber Attacks Damaging Client Trust to the Breaking Point?" July 2009, www.pwc.com/fsi

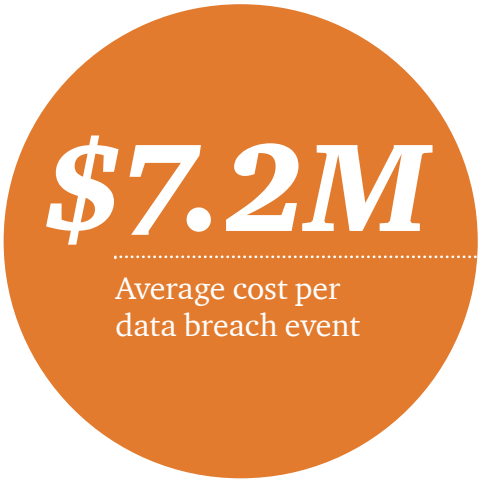
3 PwC, "2010 Mobile Security Practices Benchmarking Assessment," January 2011, www.pwc.com

4 Spence E. Ante, "Banks Rush to Fix Security Flaws in Wireless Apps," Wall Street Journal, November 2010, www.online.wsj.com

5 Ride the Lightning, "CIOS See Smartphones as Data Breach Time Bombs," November 2010, www.ridethelightning.com

6 Fishnet Security, "Survey of Security and Data Breach Trends for 2010," July 2010, www.fishnetsecurity.com

When things go wrong, the consequences—both financial and reputational—can be very real.



The real-world consequences of a data breach are significant.

- **Negative impacts on reputation and brand**—Consumer perception is a reality; any compromise of data can result in the loss of trust by customers and, with that, the loss of business.
- **Decreased revenue and profits**—Individuals care deeply about their personal information; they lose trust in institutions that fail to protect it. The recent growth in identity theft has not yet had a marked impact on key revenue streams for financial institutions—such as debit card usage and Internet payment transactions. Institutions that fail to retain customer trust will lose clients, and/or their volume of mobile transactions will be reduced.
- **Higher remediation and litigation costs**—In 2010, data breaches reached a cost of **$214** per compromised record and averaged **$7.2 million** per data breach event.[1] Insufficient data protection and privacy controls can result in significant costs for response and remediation associated with data breaches, lawsuits, government fines, and failure to comply with new regulations.

1 "Symantec / Ponemon Institute, "2010 Annual Study: US Cost of a Data Breach—Compliance pressures, cyber attacks targeting sensitive data drive leading IT organizations to respond quickly and pay more," March 2011, www.symantec.com.

Securing mobile applications is not easy. Banks are dealing with constantly evolving threats, as the security challenges they face become ever more complex.

Financial services institutions are prime targets for criminals—with global operating models, data flows to third-party service providers, and big payoffs from stolen data.

The complex structure of financial institutions and the global, interconnected marketplace in which they operate make it difficult to effectively track and manage customer data—as well as the criminals that infiltrate it.

Complicating this difficulty, the use of third-party service providers makes traditional protection methods such as perimeter controls less effective, resulting in inadequate measures to protect sensitive data. Different providers may be regulated differently and use conflicting security controls and privacy policies to secure sensitive customer information.

Threats to mobile applications are gaining sophistication.

Along with the increase in mobile-application usage, there is an alarming increase in potential malicious users whose skills mature every day that mobile applications are on the market. The following are examples of potential attacks and exploits to which mobile applications are vulnerable:

- Storage of mobile device identifiers
- Clear text capture of credentials and personal information caused by failure to encrypt data at rest and in motion
- Application-directed vulnerability exploits aimed at stored user information
- Man-in-the-middle and phishing attacks
- Session hijacking
- Transparent proxy use that allows encrypted network traffic sniffing for user credentials and for accessing sensitive information
- The use of social media and other unique threats

Leading financial institutions have made application security an integral part of their mobile-application development process. [1]

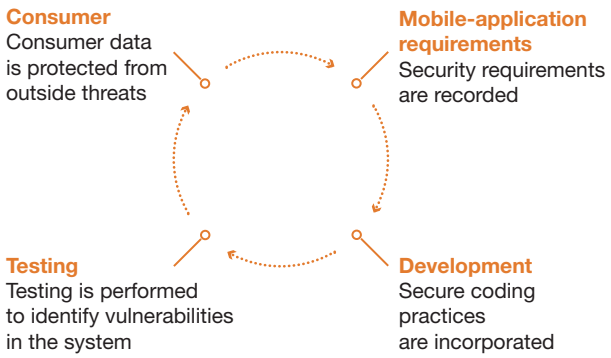
We see that leading institutions are integrating security into their application development process. This can significantly reduce the overall likelihood of identity thefts and data breaches.

With the escalation of mobile banking and payments capabilities, application developers need to adapt their processes to protect against the additional threats associated with mobile devices.

Leading institutions are following key practices that are designed to promote fraud prevention, consumer protection, and overall security for mobile-application development.

Leading institutions recognize that an appropriate defense requires a coordinated effort among corporate groups, with a focus on security, privacy, fraud prevention, and records management. Also required is a high level of cooperation and understanding—both from the business units that own the data and from the compliance department.

Integration of security with the application development process



1 PwC, "2010 Mobile Security Practices Benchmarking Assessment," January 2011, www.pwc.com.

Financial institutions are also implementing secure technologies to protect employees' mobile devices.

Before deploying mobile technology to their employees, financial institutions need to be confident that the corporate data is secure. Leading institutions are adopting a range of mobile protection technologies.

Mobile protection technologies	
Mobile Device Management (MDM)	• Secures, monitors, and manages enterprise mobile devices and can act as a proxy for device activity (such as web browsing and email), depending on the vendor solution. • Device activity is filtered, based on management defined policies. • Devices receive and execute management commands from a central server. • Vendors: AirWatch, Good for Enterprise, RIM, McAfee, MobileIron, Sybase Afaria.
Secure Application Container	• Corporate data (email, contacts, internal web sites, etc.) is encrypted within a secure application that is firewalled from the rest of the operating system. • Data transfer occurs between the mobile device and a secure application server via an encrypted channel. • Vendors: Good for Enterprise, GoodReader, BoardVantage, SAP BusinessObjects.
Device Virtualization	• Mobile devices use a hypervisor to create secure separation between underlying hardware and secure software that runs on top of it. • Device virtualization enables multiple OSs or virtual machines to segregate personal and corporate information and use. • Vendors: VMWare, Citrix.
Antivirus	• Scanning capabilities depend on the nature of the OS and the server. • Some antivirus tools are limited to scanning file attachments on the device and server, while others are capable of scanning applications, settings, data, and media files for malware. • Vendors: Lookout (Android), Intego's VirusBarrier (iOS), AVG (Android).

Industry leaders are also implementing solutions to enhance the security of customer-focused apps such as online banking, mobile banking, and mobile payments.

As consumer interest in online banking, mobile banking, and mobile payments continues to rise, we have seen leading financial institutions build customer confidence in the security of these banking options by offering various online security applications.

Online security solutions	
Encryption	• Device has OS protection options. • Developers secure application through OS encryption algorithms and protection levels. • Option exists to decrypt application data only after device is unlocked. • Encryption protects against jailbroken device threats.
Application Code Review	• Automated tools review application coding for common vulnerabilities. • Vendors: Veracode, Fortify.
Strong Authentication	• Out-of-band, multi-factor authentication (for example: email, SMS, and "image-based" challenge, where the customer selects images of objects that are predetermined upon registration). • Vendors: Confident Technologies, Visualtron's MobileKey, ArcotID.

Current situation

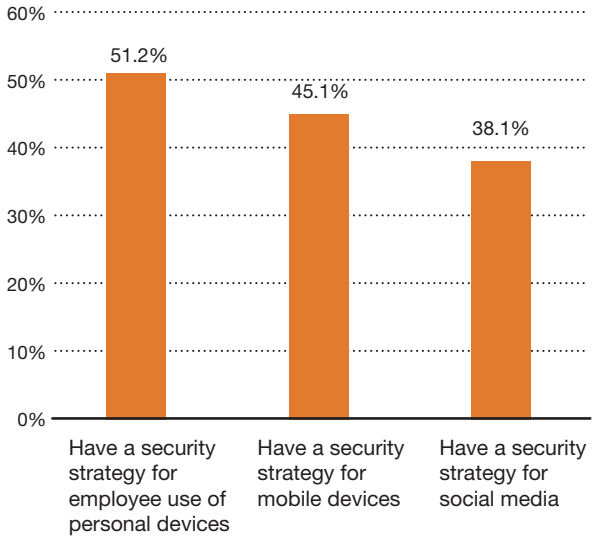
An in-depth view of the industry environment.

PwC's recent survey regarding information security underscores the need for financial institutions to consider the security needs of mobile and social media.[1]

Responses to PwC's 2012 *Global State of Information Security Survey* **underscore the need for financial institutions to improve mobile security due to the increased use of mobile devices to access data.**

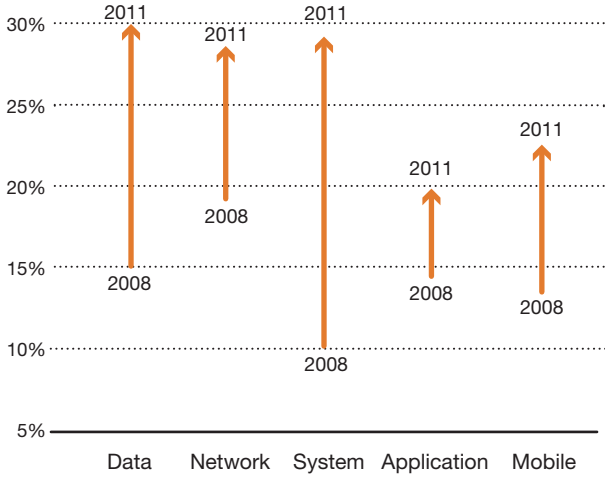
Fewer than half of the respondents have mobile and social media security strategies.

Q: "What process information security safeguards does your organization currently have in place?" (Not all factors shown; total does not add up to 100%).



Data security breaches have increased at a faster pace than any other security incident.

Q: "What types of security incidents (breach or downtime) occurred?" (Respondents were able to select more than one type of security. As a result, percentages do not add up to 100%).



1 PwC, "PwC 2012 Global State of Information Security Survey – Key findings from the 2012 Global State of Information Security," September 2011, www.pwc.com/giss2012.

According to PwC's research, the majority of security professionals expect to increase their spending on mobile security in 2012.[1]

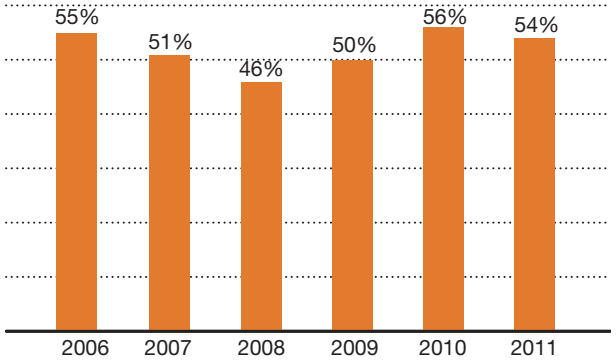
Our survey reveals a significant trend

As long as the global economy continues on its current recovery course, there is greater optimism among survey participants that security-related budgets will increase more than at any time since the financial crisis.

We see this growing optimism as an indicator of an increasing awareness among executives regarding the importance of tighter security in the mobile banking arena going forward—and those executives' corresponding needs to earmark funding for the development and implementation of effective security policies, standards, and technologies.

Security spending is expected to remain high.

Q: "When compared with last year, security spending over the next 12 months will:" (Respondents who answered "Increase up to 10%," Increase 11–30%," or "Increase more than 30%").



1 PwC, "PwC 2012 Global State of Information Security Survey – Key findings from the 2012 Global State of Information Security," September 2011, www.pwc.com/giss2012.

Financial institutions have global operating models and are therefore subject to privacy-related requirements throughout the world.

Privacy requirements differ significantly between regions, depending on whether the requirements are products of formal governmental legislation, regulatory bodies, or statutes in certain industry sectors—or whether they are driven by ad hoc circumstances.

Region	Privacy-related requirements
North America	• In **North America**, privacy requirements are the working product of a complex maze of legislation, government regulation (federal/state/province), and self-regulation (industry-specific bodies). From the SEC, the Federal Trade Commission (FTC), and the Federal Financial Institutions Examination Council (FFIEC) to industry standards such as the Payment Card Industry (PCI), many stakeholders play a role in ensuring compliance. -The **Gramm-Leach-Bliley** Act has resulted in the issuance of significant overarching rules and regulations, including the SEC's Regulation S-P and the FTC's Identity Theft Red Flags Rule. -The *Dodd-Frank Wall Street Reform and Consumer Protection Act* imposes new requirements on financial institutions regarding disaster recovery, data protection, record-keeping, and safeguarding personally identifiable information.[1] -In the United States, 46 states have instituted data breach notification statutes, some of which have provisions for fines and sanctions.[2] -The PCI Security Standards Council, a global, open-industry standards body providing management of the PCI data-security standard, recently released a new policy outlining which mobile-acceptance apps can be evaluated under its security rules.[3]
Europe	• In the **European Union**, all member states are subject to the EU Data Protection Directive. This requires each member state to transpose the Directive into governmental law, specifying the exact requirements and the scope of covered individuals or legal entities. While the internal laws in each member state vary slightly, all of the laws are consistent with the overarching Directive.
Asia-Pacific	• In the **Asia-Pacific** region, the Cross-Border Privacy Enforcement Arrangement (CPEA) was created to promote effective information privacy protection and the free cross-border flow of information. CPEA establishes a cooperative regional framework covering enforcement of privacy laws between APEC (Asia-Pacific Economic Cooperation) economies and their trading partners. However, the privacy protection requirements still lie with the individual member nations themselves and consistent regulations are being developed.
South America & Africa	• In **South America** and **Africa**, to date, few to no formal privacy-protection requirements have been enacted by legislative or regulatory bodies.

1 Dodd-Frank Wall Street Reform and Consumer Protection Act, (l) Systems Safeguards; (K) Record Keeping, 2010, www.sec.gov.

2 Digital Transactions, "PCI Council Releases 'First Step' Guidelines on Mobile-Acceptance Apps," June 2011, www.digitaltransactions.net.

3 PCI Securities Standard Council, "Payment Application Data Security Standard," October 2010, www.pcisecuritystandards.org.

Competitive intelligence

Our observations of industry practices.

IT organizations at leading financial institutions are in various stages of adopting mobile security practices to meet the challenges driven by an evolving mobile market.

Leading practice area	Top 10 North American bank	Major global bank	Retail bank
Assess current mobile-application security	• The bank demonstrated an average level of maturity for multi-factor authentication, mobile application security audit, remote server audit information, and unique firewall controls for mobile application devices. • The bank demonstrated that it was lacking in the following security areas: - Transport-level encrypted traffic - Application data-store encryption on mobile devices - Mobile intrusion detection capabilities	• The bank developed an overall approach to assessing mobile-application security by performing the following: - Provided developers with a questionnaire to be completed with input from IT infrastructure and Information Security personnel. - Generated an exception-based report, which flagged questionnaire responses that deviated from industry leading practices. - Maintained a risk register of common mobile-application risks (including risks associated with encryption, authorization, authentication, secure data storage, memory, application audit, application behavior, and mobile firewall policies). Controls to alleviate these risks were included.	• Several significant mobile security risks were identified in mobile applications that were developed for iPhone, Android, and BlackBerry devices. Risks of potential vulnerabilities that could lead to the breach of sensitive data included data stored on the device file systems, as well as within backup files created by the mobile devices.

Leading On Par Lagging

IT organizations at leading financial institutions are in various stages of adopting mobile security practices to meet the challenges driven by an evolving mobile market. (continued)

Leading practice area	Top 10 North American bank	Major global bank	Retail bank
Integrate mobile-application security into the mobile Software Development Lifecycle (SDLC)	 • The bank failed to integrate mobile-application security leading practices into the SDLC.	 • The bank confirmed that proper information-security policies and practices were implemented into the mobile-application SDLC: - Developers are responsible for eliminating any unnecessary risks from the mobile-application environment. - Where appropriate, developers receive input from IT infrastructure and Information Security personnel. - The security framework is reviewed by Information Security to determine if the application is worthy of development.	 • The bank developed its mobile-application using its standard web application SDLC rather than an SDLC that is specific to mobile applications. As a result, security issues with the mobile application could arise because concerns that are specific to the mobile environment, such as mobile device authentication and the use of jailbroken/rooted mobile devices, may not be adequately addressed.

IT organizations at leading financial institutions are in various stages of adopting mobile security practices to meet the challenges driven by an evolving mobile market. (continued)

Leading practice area	Top 10 North American bank	Major global bank	Retail bank
Strong authentication using mobile-specific information or applications	• The bank's current strategy is to leverage two-factor authentication. • Current security practices include a strong level of mobile application-specific firewall rules and traffic detection systems in order to reduce systemic risks throughout the application request cycle, including authentication.	• All applications developed by the bank (customer-facing or internal) are required to incorporate multi-factor authentication, involving a challenge question or perhaps a mobile-application-specific solution. No exchange of information between the server and mobile device may occur until the user has been authenticated within the application. Additionally, a strong "forgotten password" feature has been implemented, which considers "out-of-band" solutions for user authentication.	• The bank's mobile application uses multi-factor authentication and requires the user to answer a challenge question before granting access to the application. However, no mobile-specific information is required by the mobile application, which increases the risk of a successful mobile-based authentication bypass attack.

Leading On Par Lagging

IT organizations at leading financial institutions are in various stages of adopting mobile security practices to meet the challenges driven by an evolving mobile market. (continued)

Leading practice area	Top 10 North American bank	Major global bank	Retail bank
Encryption of sensitive information on the device	• While the bank encrypted sensitive authentication-specific information on the local device, there was a general lack of encryption of general application information that malicious users could leverage to infer sensitive information and perform an attack.	• The bank required a strong business case in order to store any application information within the mobile device file system. • No sensitive information is stored within the mobile device file system unless the application has specific approval to run locally on the device without connection to the server. • All information residing within the device file system, as well as data in transit, is encrypted according to industry-standard algorithms (e.g., AES 128 bit). Developers make correct use of public key cryptography and avoid using in-house encryption methods. • To test the effectiveness of secure data storage and encryption, Information Security personnel perform penetration tests against the application at the server and mobile device levels. These tests consider "worst-case scenarios," including a completely compromised mobile device.	• A security assessment revealed that sensitive information was being insecurely stored within cache files on the mobile device's file system.

Leading On Par Lagging

A framework for response

Our recommended approach to the issue.

When institutions carefully set their strategy for mobile banking security, they are positioned to build customer loyalty and meet the requirements of security regulations.

Case study: Mobile banking security strategy.

PwC's framework for response focuses on developing a mobile banking security strategy that meets organizational goals, including the needs to earn and retain customer loyalty and meet security regulations.

Customer loyalty is more likely to result from a successfully implemented mobile security strategy. As mobile banking use increases, it is inevitable that security breaches will gain public attention. Financial institutions that avoid the headlines will better foster a sense of trust and safety in their customers.

A well-designed mobile security strategy will incorporate leading practices in the marketplace, and innovate new practices to create competitive advantage. The leading strategies will build customer loyalty by helping reduce security breaches, and enabling greater flexibility in meeting future mobile security regulations.

Regulators are expected to give mobile banking activities increased scrutiny. To be prepared for new regulatory requirements, financial institutions will need to have a sound mobile security framework in place. Demonstrating robust security practices may also lessen regulators' zeal to impose burdensome restrictions.

Mobile security policies and standards, in combination with industry leading practices, are the key ingredients to improving mobile security.

Mobile security policies & standards

- User-to-device interaction
- Device-to-device interaction
- Device management
- Device protection
- Policy management
- Mobile applications

Like any good security program, organizations must start by defining acceptable mobile policies and standards. These standards should address the six high level categories listed on the left.

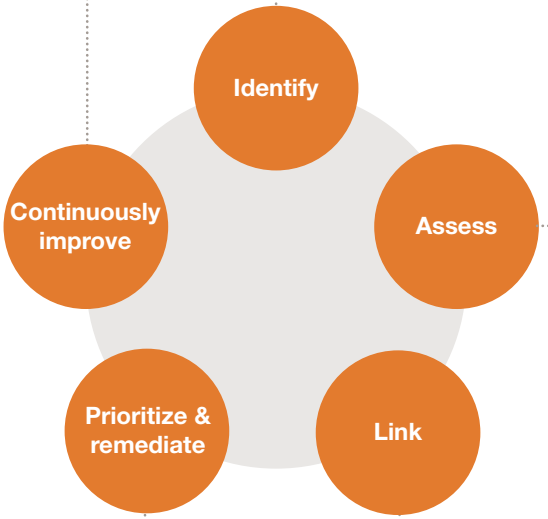
In addition, policies and standards must be supported by a number of leading practices, which include process and technology related controls. These are listed in the graphic to the right. Additional detail on each is provided on the following pages.

Mobile security leading practices

- Access to network resources
- Authentication
- Application audit
- Transport encryption
- Firewall policies
- Storage
- Authorization
- Application behavior
- Internal and external privacy policies
- Intrusion prevention
- Memory
- Software development lifecycle (SDLC)

Five-step process for improving mobile security

With the aim of protecting sensitive data, this five-step process helps financial institutions to comply with regulatory requirements and implement leading practices into the software development lifecycle (SDLC).



- Identify regulatory guidance (FFIEC/BITS).[1]
- Identify new mobile-application security leading practices, with a focus on cookie handling, encryption of sensitive information, and clearing of memory where possible.
- Identify where gaps exist between implemented controls and mobile-application security leading practices.

- Assess policy and procedural controls that are in place.
- Assess mobile application for each device platform as well as security of mobile versions of websites.
- Assess technical controls that are in place protecting key infrastructure that hosts or transmits sensitive data.
- Assess fraud monitoring and detection capabilities that are in place for transactions involving sensitive data that is specifically from mobile devices.

- Link leading practices to the SDLC.
- Develop unique intrusion detection system/intrusion protection system (IDS/IPS) rules for mobile traffic.
- Maintain firewalls specifically for mobile application traffic, and periodically perform deep inspections of mobile traffic.
- Encrypt mobile-application network traffic.
- Ensure segregation of mobile device traffic from standard network traffic.

- Perform ongoing vulnerability assessments and code reviews.
- Continuously reassess the environment for vulnerability using code reviews.

- Evaluate threats to the environment, and prioritize resulting gaps from prior workstreams to understand where the highest risk areas reside.
- Develop a remediation strategy based on threats, risks, and available spend—including potential design and the implementation of new breach protection processes or technology.
- Remediate, based on the roadmap for improving mobile security.

1 BITS (not an acronym) is the technology policy division of The Financial Services Roundtable, which focuses on improving operational practices and public policy in the financial sector.

The roadmap for improving mobile security

The mobile security framework builds upon the foundation of traditional mobile security standards and incorporates industry-leading practices. The framework includes the five-step process to help financial institutions improve their mobile security. For each policy and standard, organizations should go through the five-step process to identify the appropriate leading practices (both technical and process-related).

Mobile security policies & standards

- User-to-device interaction
- Device-to-device interaction
- Device management
- Device protection
- Policy management
- Mobile applications

All policies and standards go through the five-step process, while incorporating leading practices.

Mobile security leading practices

- Access to network resources
- Authentication
- Application audit
- Transport encryption
- Firewall policies
- Storage
- Authorization
- Application behavior
- Internal and external privacy policies
- Intrusion prevention
- Memory
- Software development lifecycle (SDLC)

Mobile security leading practices

Access to network resources

When granting access to enterprise network resources from mobile applications, institutions should consider the following:

- Secure access via VPN/SSH from mobile phone
- Secure access via HTTPS tunnel
- Policies for secure access to VPN/SSH resources from mobile traffic
- Segregation of internal network resources from mobile device traffic

Transport encryption

Encrypted information used for transmission and user session management should include the following:

- Application session encryption
- Application transport encryption
- Use of public key cryptography

Authorization

Institutions should consider the authorization controls both on their server and mobile devices.

Authentication

When establishing user authentication controls for mobile-application environments, institutions should incorporate the following:

- User/password authentication
- Multi-factor authentication
- Authentication controls for each request to server

Mobile security leading practices (continued)

Application audit

Mobile application audit information can help organizations monitor application usage trends and identify abnormal application behavior, thereby further protecting mobile-application traffic:

- Audit application initialization on mobile device.
- Secure audit information on remote server.
- Institute mobile-application audit capabilities and controls for mobile-application traffic.
- Develop unique IDS/IPS rules for mobile-application traffic.
- Encrypt audit information stored on local devices.

Application behavior

Effectively monitor application behavior:

- Develop mobile threat detection capabilities.
- Use secure cookies' handling and transmission.
- Use secure application redirects.
- Develop geo-location processes.
- Check periodically on server for new types of vulnerabilities and alerts.

Mobile security leading practices (continued)

Storage

Ensure that sensitive application information is encrypted and that there is sufficient storage capacity on the mobile device:

- Encrypt application data storage on the mobile device.
- Use secure password storage on the mobile device.
- Use secure single sign-on session storage on the server and mobile device.

Memory

Secure data in memory, and improve memory capacity:

- Secure personally identifiable information in memory.
- Protect application memory space.
- Perform fault recovery on server and mobile device.
- Perform memory clean-up on server and mobile device.
- Application transport encryption.
- Use public key cryptography.

Firewall policies

Institutions should not only deploy firewalls specifically for mobile application traffic, but also perform a deep inspection of mobile traffic.

Intrusion prevention

Institutions should not only route mobile application traffic based on threat level, but also develop unique intrusion prevention rules for mobile traffic.

Mobile security leading practices (continued)

Internal & external privacy policies

Maintain and display internal and external privacy policies within the mobile application:

- Maintain internal privacy policies for mobile devices.
- Maintain external privacy policies for mobile application users.
- Display an acceptance of personally identifiable data policy by application.

SDLC

Integrate mobile security within the SDLC:

- Establish security standards for mobile application development.
- Develop automated code review tools for mobile applications.
- Develop vulnerability assessments in development, test, and production environments.

To achieve advanced mobile security, institutions should have an SDLC that specifically addresses mobile security concerns:

- Build security into the mobile application development methodology.
- Perform penetration testing in the development and test environments to minimize security flaws in the production environment.
- Identify the unique threat vectors from mobile applications, and develop mobile threat detection capabilities.
- Build secure code analysis requirements into the mobile SDLC.

How PwC can help

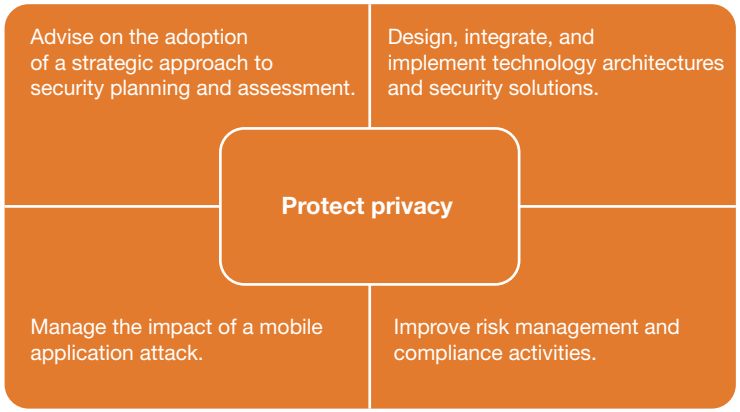
Our capabilities and tailored approach.

PwC's background

Global financial services security and privacy capabilities

PwC is the leading service firm in the financial services industry with regard to privacy and security expertise. Our Privacy and Information Security practice includes more than 1,100 professionals in the United States alone and 2,900 around the world, who are fully dedicated to information security and able to provide a broad scope of security and privacy expertise, as well as deep technical knowledge. Our practice is dedicated to providing our clients with world-class security advice, including strategy, design, implementation, and assessment services. A large, dedicated practice of this size allows us to meet regularly with the industry analysts and vendor partners to shape the future direction of the security landscape.

PwC was named as a leader in the information security and risk consulting services market, according to The Forrester Wave™. According to the independent report, PwC has significant presence and the most extensive experience in the security and risk space. We offer a balanced, yet pragmatic, approach to managing business requirements, focusing on clients as our primary objective.[1]

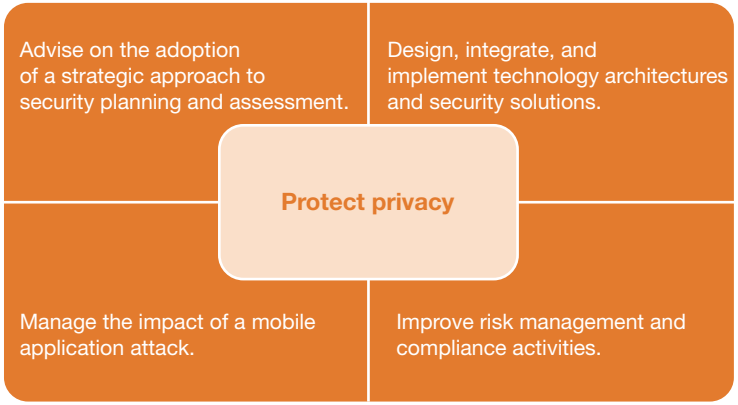


1 Forrester Research Inc, "The Forrester Wave: Information Security And Risk Consulting Services, Q3 2010," August 2010, www.forrester.com.

PwC's approach: Privacy

Protect privacy

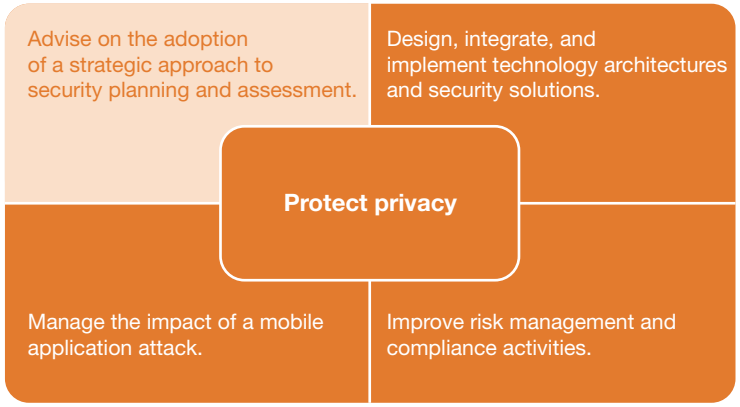
- Design and help implement privacy awareness programs.
- Enhance the reporting of privacy-related risks at the board, executive management, and task force levels.
- Perform integrated privacy and security assessments.
- Inventory and map business processes that involve high-risk data elements throughout the data life cycle.
- Help develop a third-party privacy and security oversight program with contractual safeguards, manual or automated pre-contract risk-based assessments, and an ongoing auditing program.



PwC's approach: Security planning and assessment

Advise on the adoption of a strategic approach to security planning and assessment

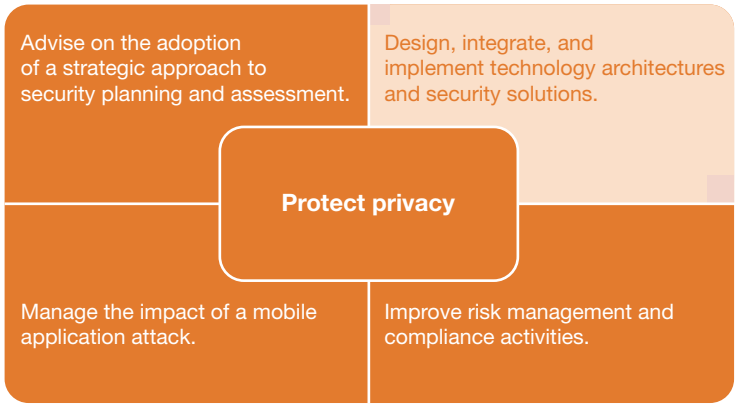
- Help clients better align security governance and planning in order to support business objectives and compliance requirements.
- Increase the ease of funding for security projects from management by communicating information along multiple dimensions.
- Help develop, communicate, and sustain a comprehensive security strategy that is actionable, repeatable, and reportable.
- To evaluate security programs, leverage PwC's SecurityATLAS™ tools and overall security taxonomy, including various capability and process models.



PwC's approach: Technology architectures and security solutions

Design, integrate, and implement technology architectures and security solutions

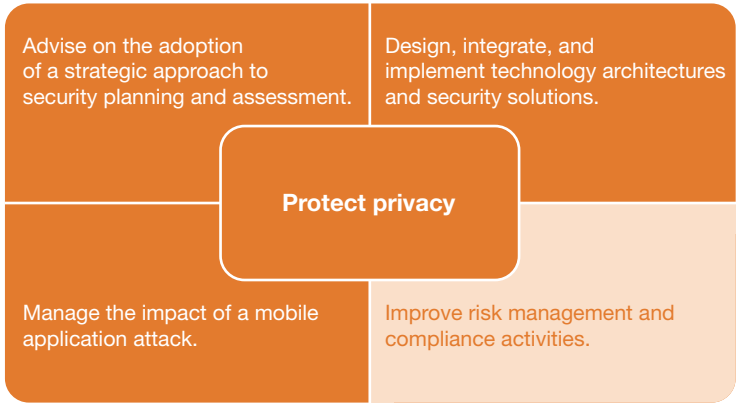
- Provide security architecture and design implementation services.
- Deliver application security as well as architecture and code reviews.
- Help design and implement identity and access management solutions.
- Design and implement integrated threat and vulnerability management solutions.
- Provide mobile security strategy, analysis, design, and assessment services.
- Help clients improve key security processes such as those supporting security communications and reporting.



PwC's approach: Risk management and compliance activities

Improve risk management and compliance activities

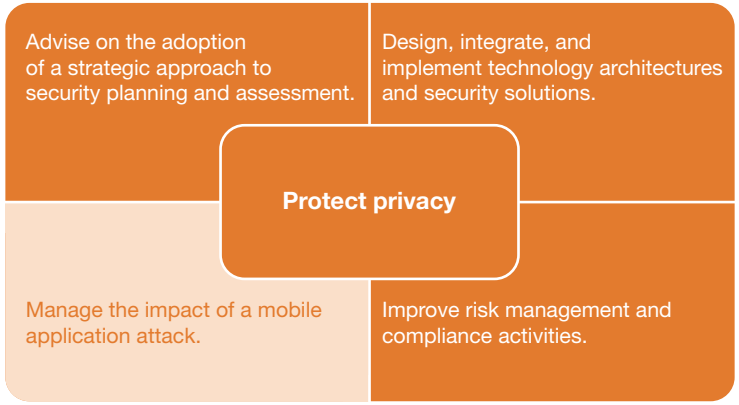
- Work with clients to identify risk areas and establish priorities for remediation.
- Use proven methodologies and deep industry knowledge to integrate security infrastructure (people, processes, and technology), and help implement standardized processes.
- Make it easier to monitor compliance with established standards and policies, and maintain asset risk exposure within a known and accepted range.



PwC's approach: Mobile security attacks

Manage the impact of a mobile-application attack

- Help companies respond to unplanned security events.
- Provide security-related crime dispute analysis and digital forensic services.
- Help define security crisis and response policies and procedures.
- Provide postmortem security services to analyze incidents and help prevent future occurrences.
- Help define security monitoring processes and incident response policies and procedures.



PwC Advisory

We look across the entire organization—focusing on strategy, structure, people, process, and technology—to help our clients improve business processes, transform organizations, and implement technologies needed to run the business.

Client needs	Issues we help clients address
Manage risk and regulation	• Building a risk-resilient organization • Managing ERP investment and project execution risk • Safeguarding the currency of business; keeping sensitive data out of the wrong hands • Ensuring capital project governance and accountability • Assessing and mitigating corruption risk in your global business operations
Build effective organizations	• Establishing effective strategic sourcing and procurement • Realizing competitive advantage through effective sales operations inventory planning • Transforming the close and consolidation process to work for you rather than against you
Reduce costs	• Driving efficiency through shared services • Redesigning finance to realize efficiency and competitive advantage • Taking control of cost through effective spend-management and cash-forecasting practices
Leverage talent	• Defining and implementing an effective HR organization • Rethinking pivotal talent
Innovate and grow profitably	• Reshaping the IT function into a source of innovation • Transforming business information to drive insight and fact-based decision making • Evaluating acquisition and divestiture strategies to position for the future • Realizing deal synergy and value • Developing sustainability programs that add value

What makes PwC's Financial Services practice distinctive

Integrated global network	With 34,000 industry-dedicated professionals worldwide, PwC has a network that enables the assembly of both cross-border and regional teams. PwC's large, integrated global network of industry-dedicated resources means that PwC deploys the right personnel with the right background on our clients' behalf, whenever and wherever they need it.
Extensive industry experience	PwC serves multinational financial institutions across banking and capital markets, insurance, asset management, hedge funds, private equity, payments, and financial technology. As a result, PwC has the extensive experience needed to advise on the portfolio of business issues that affect the industry, and we apply that knowledge to our clients' individual circumstances.
Multidisciplinary problem solving	The critical issues financial institutions face today affect their entire business. Addressing these complexities requires both breadth and depth, and PwC service teams include specialists in strategy, risk management, finance, regulation, operations, and technology. This multidisciplinary approach allows us to provide support to corporate executives as well as key line and staff management. We help address business issues from client impact to product design, and from go-to-market strategy to operating practice, across all dimensions of the organization. We excel at solving problems that span the range of our clients' key issues and opportunities, working with the heads of business, risk, finance, operations, and technology.
Practical insight into critical issues	In addition to working directly with clients, our practice professionals and Financial Services Institute (FSI) regularly produce client surveys, white papers, and points of view on the critical issues that face the industry. These publications—as well as the events we stage—provide clients new intelligence, perspective, and analysis on the trends that affect them.
Focus on relationships	PwC US helps organizations and individuals create the value they're looking for. We're a member of the PwC network of firms with 169,000 people in more than 158 countries. We're committed to delivering quality in assurance, tax, and advisory services.

Appendix

Select qualifications.

Assessment of mobile application security—Financial services organization

Issues	A financial services organization had developed a mobile banking application that customers could use to execute banking transactions from their smartphone. The client recognized the additional risks posed by the new mobile application platform in strong contrast to the standard banking Web application—specifically, the risk of "leaving behind" sensitive or personally identifiable information on the smartphone.
Approach	PwC worked closely with the client's team to develop a mobile-application testing methodology that included a full scope of penetration testing activities. This methodology took into account the various attack vectors facing the mobile application, and included testing the application's security from the perspectives of using the application, with a standard browser, and from the mobile device itself. Additionally, PwC developed a mobile application security questionnaire and solicited feedback from leading organizations within the client's industry. Using these results, PwC was not only able to benchmark the client's mobile security practices against its industry peers, but also to identify the mobile security practices of leading organizations.
Benefits	PwC identified several ways in which the client could improve its mobile-application security practices to address the additional risks posed by the new mobile application platform. The results of the benchmarking assessment allowed the client to identify strengths and weaknesses within its mobile security practices and to initiate process improvements.

Assessment of payment system application—Major central bank

Issues

A major central bank was in the midst of a multi-year program aimed at migrating its large-value ($3 trillion average daily transfer value) and time-critical payment systems from a legacy mainframe-based application to a distributed platform architecture. The bank required identification of any critical flaws in the overall design of the distributed architecture. Also paramount was evaluation of whether the design addressed the business requirements in terms of performance, scalability, resiliency, availability, and reliability. Furthermore, the bank needed to identify if the complexity of the design posed any risk and how to mitigate these risks.

Approach

PwC proposed conducting a systematic evaluation of the proposed system architecture and technical design. We leveraged assessment toolkits and accelerators that enabled evaluating the application capabilities against the architectural dimensions. The architecture assessment toolkit enabled measurement of strengths of the target platform across a set of weighted criteria. The criteria were assessed across the categories of performance and scalability, resiliency, quality assurance processes, tools testability, and test coverage. The technical design was evaluated across the dimensions of application architecture/design, application integration capabilities, data architecture and design, and infrastructure and deployment architecture.

PwC employed a collaborative approach that allowed us (1) to have a better understanding of the bank's business requirements and service level agreements (SLAs) that the application architecture would need to adhere to and (2) to understand the rationale employed behind the architecture and design in meeting the SLA. We thereby obtained, and agreed upon, a common understanding of the issues, risks, and recommendations identified.

Benefits

The overall architecture was validated against business requirements, available solutions, leading practices, and design patterns applicable to the architecture. PwC provided a final executive presentation to leadership, along with a summary of the assessment highlighting the key risk areas with a clear set of remediation steps that was incorporated into the system implementation roadmap.

Online banking channel assessment—Top 10 US bank

Issues	Leadership of a leading regional bank was expecting significant growth to reach industry parity in household adoption for both online banking and bill pay. Recent application upgrades supporting the online banking channel were not seamless. Various issues were encountered while deploying the application to production. Bank leadership determined it was prudent to perform a comprehensive review of the people, processes, and technologies required to enable the online banking channel.
Approach	PwC proposed conducting a comprehensive review of the online banking applications across the people, processes, and technologies, including key focus areas of the project, program, and portfolio management; business requirements analysis and definition; architecture and design; development; testing; deployment and release management; support help desk; and security and risk. PwC followed a collaborative approach to conduct interviews and review artifacts to obtain a better understanding of the people, processes, and technologies of the online banking channel. Over 120 artifacts were analyzed and more than 15 interviews were conducted.
Benefits	The assessment, which was organized by the people, processes, and technologies, resulted in the identification of critical and actionable areas for improvement. PwC developed a detailed final report outlining a list of issues and their impacts, remediation options, and a roadmap to address the issues within the organization. In addition, our team created prioritized project initiatives to meet short-and long-term business objectives, and provided target organizational structure and resource requirements, as well as key performance indicators to measure the software development lifecycle performance.

Online banking future architecture and roadmap—Top 10 US bank

Issues	The bank was embarking on a large-scale platform refresh of the online banking experience, including application, banking portal, retail banking, and money movement platforms. The future state presented a new business strategy and architecture, as well as an architectural overhaul of the back-office integrations. Key challenges included adopting a unified platform assessment model that was agreeable to all business and technology stakeholders, creating a process and model to assess impacts to the overall total cost of ownership, composing the desired state technology architecture, and assuring the migration strategy to the end-state.
Approach	PwC worked closely with the client to develop a balanced scorecard in assessing the prevailing tools, technologies, and platforms relevant to the online banking platform functions. Our team assessed build-buy-renew options for online banking, money movement, search, targeted marketing, and niche functions such as chat/co-browse. Through discussions with various vendors, client technology, and business organizations, we then developed the desired state architecture and the migration/co-existence strategy. Using this information, PwC was able to develop the overall cost comparison model for the various platform architectures.
Benefits	The overall assessment and the associated approach provided the bank with a consistent and comprehensive result that was conclusively accepted across the technology and by the business stakeholders. The assessment not only drove the decision of a unified retail banking and money movement platform, but also assisted in the formulation of the final presentation to the executive team in finalizing the selection and obtaining sign-off on the selected software.

Mobile payments strategy—Leading US financial services company

Issues	The financial services company viewed mobile payments as both an opportunity and a threat to its core card business. The client desired an understanding of the existing space not only to defend current market share, but also to carve out a specific niche and create new value. Further, the client was concerned with its ability to quickly and effectively deploy mobile payment products. PwC was engaged to provide recommendations on which threats to mitigate, opportunities to pursue, population segments that offered greatest value, and how to make the current infrastructure more agile and relevant to the evolving mobile payment space.
Approach	PwC evaluated key leading practices in the industry to isolate trends and identify potential future-state scenarios (open platform, mobile network operator-based, etc.). PwC provided counsel on opportunities and threats, as well as which mobile payment value-added services the client should pursue.
Benefits	PwC identified US population segments that would be of the greatest value and relevance for the client's mPayment goals, and provided a number of infrastructure improvements to achieve competitive agility. By the end of the engagement, the client had begun to implement several of the recommendations, to engage partners, and to mobilize internal resources.

Mobile banking strategy—Leading US financial services company

Issues

The current mobile banking offerings of a leading financial services company were lagging behind the competition. The client was seeking to transform itself into a "thin branch" banking model, and was concerned with current infrastructure, vendor relationships, and delivery capabilities.

To catch up with the market and begin progression toward the "thin branch" model, the client sought an understanding of which mBanking features it should build, and why. To improve infrastructure and delivery, the client desired a clear assessment of the current state and recommendations for achieving future state goals.

Approach

PwC was engaged by the client's digital team to create a mobile banking strategy that included infrastructure and customer segmentation recommendations. PwC developed an mBanking landscape overview that defined baseline functionalities, key players, and consumer adoption trends. In addition to conducting a comprehensive gap analysis of current offerings, PwC provided competitive "parity" and offered tailored recommendations.

Also, PwC identified US population segments that would be of the greatest value and relevance to the client's mBanking pursuits.

Benefits

PwC defined critical milestones toward enabling a successful "thin branch" model, including a comprehensive list of required features and potential future-use cases. The team also helped to develop a current-state assessment that identified opportunities across systems, processes, security, vendors, and delivery.

Mobile application framework and enterprise device management—Large US commercial bank

Issues

A large US commercial bank wanted to standardize the process of approving mobile applications for development. This involved analyzing the business, technology, and information security impact of a mobile application that was seeking development.

The same client needed help with implementing a *Good for Enterprise* environment, in which sensitive corporate information is safely secured on personal smartphone devices in this application.

Approach

The client asked PwC to develop a risk register and developer questionnaire in an attempt to determine where the SDLC deviated from industry leading practices. The client also asked PwC to perform an assessment of the *Good for Enterprise* environment.

In response, PwC established a risk register, questionnaire, and mobile application development considerations using firm-wide and external research materials. We then executed the framework in two use-case scenarios for applications seeking development.

PwC performed a gap analysis that benchmarked the bank's *Good for Enterprise* configuration settings against industry standards, *Blackberry Enterprise Server* settings, the parent bank's settings, and other applicable standards. The team then performed a penetration test against the application on the device—analyzing data storage, memory dumps, jailbreak checks, network traffic analysis, authentication, authorization, and application auditing.

Finally, PwC recommended application infrastructure diagrams, industry mobile device management trends, and considerations for mobile application development, IT infrastructure, and information security practices.

Benefits

PwC identified security configuration settings within the *Good for Enterprise* servers that the client had not configured properly. By enabling these security settings, the client improved the security of the mobile application environment. This enhanced awareness resulted in the early identification of potential mobile security vulnerabilities and fewer such vulnerabilities making their way into mobile apps on production servers.

Mobile application security assessment—Large bank and credit card organization

Issues	A large bank and credit card organization wanted to assess its mobile banking application security. Given that its competitors were recently criticized in reputable publications for insecure storage of sensitive personal information on their applications, this bank/credit card organization wanted to ensure that it would not suffer similar reputational harm.
Approach	PwC tested the application's security at the following areas: data storage, authentication, authorization, access to network resources, and session management. The team installed various tools to upload the application folder and device file system of iPhone and Android devices hosting the application to a laptop, and performed automated and manual searches for sensitive user information for provided test accounts. PwC then ran application traffic through a transparent proxy for analysis.
Benefits	PwC identified sensitive customer information stored in an insecure manner on mobile devices. As a result, the client was able to take corrective action before the mobile application was published; therefore, no customer information was exposed. The client was also able to increase the security awareness of its mobile development team, using our work as a case study. This enhanced awareness resulted in the early identification of potential mobile security vulnerabilities and fewer such vulnerabilities making their way into production mobile apps.

www.pwc.com/fsi

To have a deeper conversation, please contact:

John Garvey	john.garvey@us.pwc.com +1 646 471 2422
Joseph Nocera	joseph.nocera@us.pwc.com +1 312 298 2745
Andrew Toner	andrew.toner@us.pwc.com +1 646 471 8327
Shawn Connors	shawn.joseph.connors@us.pwc.com + 1 646 471 7278
Christopher Morris	christopher.morris@us.pwc.com + 1 617 530 7938
Kelly Kitsch	kelly.a.kitsch@us.pwc.com + 1 312 298 2121
Stephen Russell	stephen.j.russell@us.pwc.com + 1 203 539 3079

"Gaps in the Apps: Why the Traditional Security Lifecycle No Longer Works," PwC FS Viewpoint, April 2012, www.pwc.com/fsi

LA-12-0206