FORRESTER®

For: Security &
Risk Professionals

Assess The Maturity Of Your Mobile Security Program

by Stephanie Balaouras and Tyler Shields, January 22, 2015

KEY TAKEAWAYS

The Mobile Security Maturity Model Helps Assess Your Current State

The Forrester Mobile Security Maturity Model distills the recommended functions and components of a comprehensive program into a single framework. With a three-tiered hierarchy, it also offers a methodology for evaluating the maturity of each component of the framework on a consistent and prescriptive maturity scale.

Include Others And Assess Often

Performing a maturity assessment is not a one-time exercise that you perform in isolation. You must: 1) get input from business and technology management colleagues; 2) establish a baseline, and set realistic targets; 3) measure progress at frequent and regular intervals; and 4) schedule frequent conversations with stakeholders.

Assess The Maturity Of Your Mobile Security Program

Assessment: The Mobile Security Playbook

by Stephanie Balaouras and Tyler Shields
with Laura Koetzle, Christopher Voce, Christian Kane, Chris Sherman, and Jennie Duong

WHY READ THIS REPORT

When developing a mobile security strategy for today's digital business, security and risk (S&R) executives must consider both how they will enable a digital workforce that expects to work anytime and anywhere, and how they will secure their customers' mobile moments — all without compromising their employees' or their customers' mobile experiences. In response to those challenges, we designed the Forrester Mobile Security Maturity Model. The model is a comprehensive framework that S&R leaders can use to identify the gaps in their mobile security program, evaluate its maturity, and determine how they can play a much bigger role in their firm's overall mobile strategy. The model consists of four top-level domains, 14 functions, and 50 components, each with detailed assessment criteria. It provides a consistent and objective method for evaluating security programs and articulating their value. This is an update of a previously published report; Forrester reviews and updates it periodically for continued relevance and accuracy.

Table Of Contents

Notes & Resources

Forrester incorporated feedback from numerous end user and vendor interactions as well as various other client engagements.

Related Research Documents

The Forrester Mobile Security Maturity Model
January 22, 2015

TechRadar™: Enterprise Mobile Security, Q4 2014
November 3, 2014

It's Time To Level Up Your Mobile Application Security Program
August 26, 2014

YOU CAN'T DEVELOP A STRATEGY WITHOUT UNDERSTANDING WHERE YOU ARE

Mobility is already revolutionizing end user computing and customer experience. Thus, it's no surprise that securing and supporting mobility is a top priority for the security and risk (S&R) team. However, many of our clients tell us that although they've already deployed multiple security controls and other technologies, they lack an overall strategy and have yet to define a long-term road map to reach higher levels of maturity and build advanced capabilities. They also tell us that they struggle to communicate their role and value both to employee mobility initiatives and to customer-facing mobile engagement programs. In fact, in many cases, S&R pros are not even a part of the ideation, design, engineering, and analytics of the customer-facing mobile strategy. Forrester developed the Mobile Security Maturity Model to meet those challenges. The maturity model will provide the foundation for Forrester's mobile security maturity assessment engagements as well as provide clients with a comprehensive self-assessment tool.

The Maturity Model Helps You Assess And Communicate Your Current State

Before you can develop your mobile security strategy and define your five-year technology road map, it's critical to compare the maturity of your current initiatives and capabilities with recommended best practices.[1] Forrester's Mobile Security Maturity Model will help S&R leaders:

- **Articulate the role of S&R in mobility.** Mobility is an enterprisewide initiative — it'll involve everyone from your CMO and CIO to your procurement specialists and customer service representatives. Therefore, you'll need to be able to clearly define and articulate the functions and responsibilities of the S&R team. S&R leaders must persuade the rest of the firm that the S&R team has a critical role to play in both the workforce enablement and customer engagement aspects of mobility. And that's where Forrester's Mobile Security Maturity Model comes in — it's a powerful tool for laying out functions and responsibilities and, above all, for communicating the value that you're delivering.

- **Identify gaps and develop remediation plans.** This model will help you identify areas of weakness and improvement compared with recommended best practices. Once you've identified any gaps, you can then prioritize remediation plans to make sure all components of your program are meeting your baseline expectations.

- **Show that your program improves over time.** Keeping track of operational metrics such as "percentage of employees that have BYOD support" or "percentage of sensitive customer data leaks via mobile access" is useful for identifying problem areas. However, chief information security officers (CISOs) must demonstrate that the effectiveness and maturity of their mobile security programs increase over time. The model will help you fight for budget and build relationships with the business by giving you the ability to demonstrate improvement in specific mobile security functions.

USE THE MATURITY MODEL TO DEFINE, MEASURE, AND IMPROVE

The Forrester Mobile Security Maturity Model distills the recommended functions and components of a comprehensive program into a single framework. With a three-tiered hierarchy, it also offers a methodology for evaluating the maturity of each component of the framework on a consistent and prescriptive maturity scale.

Four Domains Provide A Balanced View Of Your Program And Strategy

Our model consists of 50 components of a successful mobile security program. We then organized these into 14 functions, which we then further collected into four domains. Forrester's four domains are consistent in all of our information security maturity models (see Figure 1):[2]

- **"Oversight" helps you plan, govern, and optimize.** S&R professionals often focus on technology when it comes to mobility. They go straight to questions such as "What enterprise mobile management (EMM) tool should I deploy?" and "Should I care about mobile malware?" Thus, the oversight domain ensures that the mobile strategy and technology road map reflects business requirements and that the S&R team is a full participant in the mobile steering committee. This domain addresses the strategy, ongoing strategy optimization, and policy management functions.

- **"Technology" includes the functions for securing mobile apps, data, and devices.** Because technology is often seen as the most definitive or visible domain of mobile security, S&R pros will be surprised to find that it is still deficient. Forrester finds that many technology management organizations have focused too much on deploying specific point products and too little on the ability to deliver specific mobile functions or services to the business. It's not just about employee-owned versus company-owned devices, it's about delivering a comprehensive bring-your-own-device service that supports employee productivity.[3] In the case of customer-facing mobile, it's about protecting customers from fraud, identity theft, and privacy violations via security controls that remain as invisible as possible to the user. This domain covers the major technology functions and components for mobile security, management, and compliance.

- **"Process" refers to functions that rely on repeatable workflows with other tech functions.** Because mobility is an enterprisewide initiative, the S&R team has to work effectively with multiple groups inside and outside of the CIO's organization. This domain covers how S&R will influence, integrate with, and support the mobility efforts of the sourcing and vendor management, application development, infrastructure and operations (I&O), and customer experience teams.[4]

- **"People" describes the functions necessary for handling staff and communication.** Mobility requires S&R teams to acquire new skills and has the potential to change staffing levels and organizational structure. Mobility will also require continuous communication with business stakeholders, employees, and customers on value, policy, and security awareness. This domain covers staffing, organizational structure, user awareness and training, and communication at various levels inside and outside the technology management organization.[5]

Figure 1 The Forrester Mobile Security Maturity Model

Oversight
Strategy
Strategy development
Alignment to business strategy and objectives
Cross-functional mobile steering committee
Technology road map
Strategy optimization
Performance management (metrics)
Benchmarking
Policy management
Policy creation
Policy maintenance
Technology
Enterprise mobile management
Mobile devices management
Mobile applications management
Reporting and analytics
Enterprise mobile security
Mobile app security
Remote access/network security
Network access control
Antimalware
URL filtering
Antitheft
Selective wipe
Privacy control/mobile app reputation services
Employee authentication and identity management
Certificate management
Secure file sharing and collaboration
Data security
Archiving
Technology integration
Integration with IT service management
Integration with client/endpoint management
Customer mobile security and privacy
Customer authentication and identity management
Embedded mobile app security

61572 Source: Forrester Research, Inc. Unauthorized reproduction or distribution prohibited.

Figure 1 The Forrester Mobile Security Maturity Model (Cont.)

Process
Sourcing and vendor management
Sourcing strategy
Vendor and contract management
Incident management and forensics
Incident response
Forensics
Secure mobile app development
Software development life cycle (SDLC)
Mobile static and dynamic code analysis
Application hardening
Pen testing/third-party assessment
Developer security training/awareness
Employee mobile experience
Bring-your-own-device (BYOD) support
Employee troubleshooting and support
Employee self-services
Employee segmentation/mobile moment audit
Global support
Employee satisfaction
Customer mobile experience
Customer mobile moment audit
Customer self-services
People
Communication
Advocacy and marketing
Training and awareness
Security organization
Security staffing
Organizational structure
Training/certification
Security designers

61572 Source: Forrester Research, Inc. Unauthorized reproduction or distribution prohibited.

Use The Self-Assessment To Establish An Objective View Of Your Current Maturity

Several characteristics differentiate the Forrester model and its structure (the domains, functions, components, and maturity evaluation scale). Most importantly, the Forrester model is:

- **Objective.** Vendor and service provider biases plague many similar efforts. This model represents our unbiased advice based on extensive research to identify the characteristics and best practices of a successful mobile security program.
- **Consistent.** For the maturity model to work, it must measure each component in the same way. Forrester based its evaluation scale on the COBIT 4.1 maturity level definitions, which are: 0 — nonexistent; 1 — ad hoc; 2 — repeatable; 3 — defined; 4 — measured; and 5 — optimized (see Figure 2).[6]
- **Prescriptive.** The characteristics required to achieve the next higher level of maturity for each component are clear and distinct. An assessment should yield similar results regardless of who conducts it, and the requirements to reach the next level of maturity should be easy to understand.
- **Process-oriented.** Even for mobile security functions that primarily rely on technology, the model evaluates the processes used to choose, deploy, monitor, and manage that technology and to deliver the necessary function or service to the business. For example, we don't assess whether you have deployed a specific mobile application management (MAM) tool but whether your implementation delivers the ability to manage devices appropriately. Focusing too much on products or tools would render the assessment — and thus the results — irrelevant in a few years' time.
- **Modular and flexible.** We intentionally designed the model so that you can either deploy it as a single holistic assessment or use each of the four domains, 14 functions, and 50 components as a standalone maturity evaluation for a specific area. For example, if your firm has decided that it will not support employee-owned devices, you can set the weight of all the criteria related to BYOD to zero. Having this flexibility enables you to fit this model to your organization.
- **Uncomplicated.** Security and technology management teams must constantly respond to auditors, regulators, business partners, and other stakeholders who are conducting different types of assessments. Forrester's maturity assessment does not require extremely large amounts of background data or extracts from management tools. You can complete the assessment and evaluation based on discussions, interviews with stakeholders, and observations.

Figure 2 Forrester Maturity Level Definitions

Level	Characteristics
0 — Nonexistent	Not understood, not formalized, need is not recognized
1 — Ad hoc	Occasional, not consistent, not planned, disorganized
2 — Repeatable	Intuitive, not documented, occurs only when necessary
3 — Defined	Documented, predictable, evaluated occasionally, understood
4 — Measured	Well-managed, formal, often automated, evaluated frequently
5 — Optimized	Continuous and effective, integrated, proactive, usually automated

61572 Source: Forrester Research, Inc. Unauthorized reproduction or distribution prohibited.

WHAT THE MATURITY MODEL CAN'T AND CAN DO

As with any tool, the Forrester Mobile Security Maturity Model can only do so much. Before you begin, set reasonable expectations for what it can and can't help you accomplish. Here's what the framework cannot do:

- **Determine whether you're secure.** The purpose of the model is to evaluate the maturity of mobile security functions, including to what extent they are repeatable, documented, and measured. Conducting an evaluation with this maturity model will not tell you whether your controls are well-designed or effective. For example, it's possible for an organization to have strong security controls that are ad hoc or informal, which would earn low maturity scores. And conversely, it's also possible for a firm to earn Level 4 controls with well-documented, managed, formal, but weak controls.

- **Demonstrate compliance.** Reaching a high level of maturity in itself is not evidence of compliance. Although we believe that using this model will help you improve your security posture and compliance with many regulations, you still need to map the model's components to various regulations and standards and perform the necessary control tests to demonstrate compliance.

RECOMMENDATIONS

TO GET THE MOST OUT OF THE MODEL, INCLUDE OTHERS AND ASSESS OFTEN

To get the most out of this tool, you must embed it into your ongoing operations. Performing a maturity assessment should not be a one-time, isolated exercise. Here are a few key tactics to keep in mind:

- **Get input from business owners and technology management colleagues.** Conducting an evaluation yourself or with a small number of close team members will limit how much you learn from the exercise. Ask relevant functional and business owners inside and outside of the S&R team to participate, even if they can only assess a limited number of areas. Colleagues in application development and in the marketing, customer experience, and eBusiness roles are particularly important to include when assessing your customer-facing mobile security maturity.

- **Establish a baseline, and set realistic maturity level targets.** For the vast majority of S&R organizations, targeting a Level 5 maturity score for every component of the model won't be practical or advisable. With that in mind, S&R leaders should examine the initial results to identify unacceptable maturity gaps (e.g., places where you're at Level 1 and your prospective customers tell you that they expect you to be at Level 3) and areas where you can easily improve. Consider aspects of risk, budget, compliance, and corporate priorities to determine the level of maturity that would be appropriate for each component.

- **Measure progress at frequent and regular intervals.** Because business, employee, and customer requirements for mobility as well as the technology itself change so quickly, Forrester recommends that you assess your mobile security maturity every six months. If every six months isn't practical for your S&R team, you can extend the timeline — you should prioritize defining and adhering to a regular assessment schedule to measure progress over time. This is important for demonstrating the value of both your mobile security investments and the model itself.

- **Connect frequently with stakeholders from across the business and technology management.** The maturity model describes all of the functions and components of a mobile security program, allowing you to explain to your business and technology management colleagues the breadth of functions involved. Whenever you update your self-assessment, sit down with key stakeholders to review the results. This will allow you to highlight the strides you've made, communicate the valuable role you play in mobility, get commitment from stakeholders whose help you need to close the agreed-upon security maturity gaps, and help justify further investment.

ENDNOTES

[1] For a definition of use cases, business value, and outlook for the 15 technologies that comprise the core enterprise mobile security technologies, see the November 3, 2014, "TechRadar™: Enterprise Mobile Security, Q4 2014" report.

[2] For example, Forrester's overall Information Security Maturity Model consists of those four top-level domains, 25 functions, and 128 components, each with detailed assessment criteria. See the October 6, 2014, "The Forrester Information Security Maturity Model" report.

[3] In Forrester's 27-criteria evaluation of enterprise mobile management vendors, we identified the 15 most significant MDM providers — Absolute Software, AirWatch by VMware, BlackBerry, Citrix, Good Technology, IBM, Kaspersky Lab, LANDesk, McAfee, MobileIron, SAP, Sophos, Soti, Symantec, and Trend Micro — and researched, analyzed, and scored them. For more information, see the September 30, 2014, "The Forrester Wave™: Enterprise Mobile Management, Q3 2014" report.

[4] For more information on mobile app development best practices, see the April 30, 2014, "Address The Top 10 Nontechnical Security Issues In Mobile App Development" report.

[5] It's Forrester's view that every CIO's organization must pursue a dual agenda consisting of business technology (BT) — the technology, systems, and processes to win, serve, and retain customers — and information technology (IT) — the technology, systems, and processes to support and transform an organization's internal operations. Forrester calls this dual agenda (and the organization that supports it) "technology management." See the June 4, 2014, "Develop Broad Tech Management Capabilities In Order To Accelerate Your BT Agenda" report.

[6] Forrester uses these same maturity levels consistently in all our information security maturity models. See the December 12, 2014, "Assess Your GRC Program With Forrester's GRC Maturity Model" report and see the October 2, 2013, "The Forrester GRC Maturity Model" report.

FORRESTER®

About Forrester

A global research and advisory firm, Forrester inspires leaders, informs better decisions, and helps the world's top companies turn the complexity of change into business advantage. Our research-based insight and objective advice enable IT professionals to lead more successfully within IT and extend their impact beyond the traditional IT organization. Tailored to your individual role, our resources allow you to focus on important business issues — margin, speed, growth — first, technology second.

FOR MORE INFORMATION

To find out how Forrester Research can help you be successful every day, please contact the office nearest you, or visit us at www.forrester.com. For a complete list of worldwide locations, visit www.forrester.com/about.

CLIENT SUPPORT

For information on hard-copy or electronic reprints, please contact Client Support at +1 866.367.7378, +1 617.613.5730, or clientsupport@forrester.com. We offer quantity discounts and special pricing for academic and nonprofit institutions.

Forrester Focuses On Security & Risk Professionals

To help your firm capitalize on new business opportunities safely, you must ensure proper governance oversight to manage risk while optimizing security processes and technologies for future flexibility. Forrester's subject-matter expertise and deep understanding of your role will help you create forward-thinking strategies; weigh opportunity against risk; justify decisions; and optimize your individual, team, and corporate performance.

« **SEAN RHODES,** client persona representing Security & Risk Professionals