FORRESTER®

FOR SECURITY & RISK PROFESSIONALS

Build A Cross-Functional Mobile Security Team

Organization: The Mobile Security Playbook

by Chris Sherman

February 22, 2017

Why Read This Report

As security leaders look to support business engagement with customers, partners, and employees through mobile, they often discover gaps in team expertise. To better organize talent, security execs must divide mobile security responsibilities among existing security operations and architecture roles, They must also partner with the office of the CIO and business leaders on strategic initiatives. The goal is to build a cross-functional group of security strategy and ops staff with clear responsibilities. This report explains the elements of an effective mobile security team.

Key Takeaways

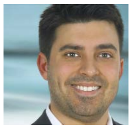
Collaborate, But Define Responsibilities For Security And Operations Staff
Ensure that your security team supports positive mobile experiences by exposing them frequently to the demands of your workforce and customers. Start by building lists of your employees' most frequent and sensitive mobile moments.

Mobile Security Skills Need To Evolve With New Technologies
Forward-leaning organizations hire security architecture and operations staff that can treat mobile capabilities holistically within the context of an organization's device and app ecosystem. Deep technical expertise in any one form factor or operating system is less desirable, especially as organizations employ a greater number of hosted security services.

Hiring Managers Must Look For Hard And Soft Skills When Recruiting Mobile Pros
While few mobile-security-specific roles exist today outside of application development, many security architecture and operations staff members will need to be generalists with an understanding of both the security and organizational implications imposed by mobile devices and apps.

Build A Cross-Functional Mobile Security Team

Organization: The Mobile Security Playbook



by Chris Sherman
with Christopher McClean, Stephanie Balaouras, Salvatore Schiano, and Peggy Dostie
February 22, 2017

Table Of Contents

Related Research Documents

Evolve Your Organization Structure To Promote Digital Maturity

Navigate The Future Of Mobile Security

TechRadar™: Mobile Security, Q1 2016

FORRESTER®

Forrester Research, Inc., 60 Acorn Park Drive, Cambridge, MA 02140 USA
+1 617-613-6000 | Fax: +1 617-613-5000 | forrester.com

Security Teams Struggle To Meet Mobile Skills And Staffing Needs

In the early days of enterprise mobility, BlackBerry and Microsoft ActiveSync were the primary mobile conduits for giving employees access to corporate email outside of the office. Mobile security responsibilities often resided with the email security team, treating mobile support as an isolated project with limited scope. Additionally, customer-facing mobile security either was nonexistent or excluded security teams from the app development table.

The continued adoption of diverse mobile devices and a multitude of apps has changed the business environment irrevocably. Employees now require mobile access to business applications, collaboration tools, and other technology assets, which has the potential to expose sensitive corporate data to theft and abuse. As a result, security teams have had to adapt their skills and staffing requirements to the changing demands placed on security by this new landscape of rapid innovation. In Forrester's latest security survey, 70% of global security technology decision-makers said that improving mobile security capabilities and services is a high or critical priority for their enterprise firm over the next year.[1] As the director of IT at a hospitality and leisure company said, "Ensuring corporate network and data security is critical, particularly now that we officially support a BYOD program for mobile devices. Addressing security issues associated with these devices and applications is important."[2] Unfortunately, mobile security capabilities have languished in most organizations for a variety of reasons:

› **Mobile security responsibilities lack definition.** Businesses need mobile expertise in multiple areas of the business outside of the security operations team, ranging from application development and line-of-business leaders to procurement and legal professionals. With new mobile apps entering the corporate ecosystem all the time, organizations have struggled to define exactly how to delegate mobile security responsibilities. For instance, one large pharmaceutical company told Forrester, "We used to have dedicated mobile security professionals, but this simply doesn't work today considering the large number of mobile projects spanning the organization."

› **Security teams don't always have the right skills.** Mobile trends such as device proliferation, the internet of things (IoT), BYOD, and the explosion of unsanctioned apps in the enterprise with access to corporate data all have serious security implications, and as a result, employees need a unique combination of skills to tackle them head-on. However, our 2016 data shows that 65% of security decision-makers at enterprise firms feel the unavailability of security employees with the right skills is a challenge or major challenge.[3] Considering that this dearth of talent will likely continue for some time, recruiting new security staff with the right expertise will be an ongoing challenge for most organizations.

› **Traditional security struggles to support business innovation, customer engagement.** According to a 2016 Forrester survey, information workers use various devices, including laptops (69%), smartphones (70%), and tablets (35%), at least weekly for work.[4] Unfortunately, many security teams today are not involved enough in supporting these employees, especially the ones that drive top-line business growth. If the security team can't deliver solutions that empower customer-facing roles and improve overall customer engagement, business functions such as sales, marketing, research, and development will acquire and deploy mobile services without consulting the security team.

› **Some security teams treat mobile as just another endpoint.** As mobile use has increased, organizations have sought ways to simplify the security and management of these devices. One way is to assign mobile management and security ops to the same staff handling traditional endpoints (e.g., laptops, desktops). Vendors have supported this with technologies that integrate mobile, laptop, and desktop security tools within unified policy engines.[5] This has pushed some teams to treat mobile as just another endpoint. However, because more and more mobile endpoints are personally owned, device-centric control is a mistake. Mobile security is its own distinct function, and security teams need to focus on securing apps and data, rather than devices. Today, security teams need fewer staff with device-specific skills.

> "Ensuring corporate network and data security is critical, particularly now that we officially support a BYOD program for mobile devices."

Develop Integrated, Cross-Functional Mobile Security Expertise

Mobile security must operate at the same level of flexibility and agility that the business does — or risk becoming an impediment to innovation. To do so, a clear assignment of responsibilities with well-defined channels of collaboration both within and outside of security is a must (see Figure 1). This means building a virtual mobile security team made up of security and operations staff. Today, the most successful mobile security strategies build on a core set of security responsibilities:

› **The vulnerability management team operates in lockstep with mobile-threat research.** Existing vulnerability management teams manage mobile vulnerabilities and exploits alongside traditional endpoints. However, they must cooperate with the security staff responsible for identifying and researching mobile threats in the wild. This will give the vulnerability management team greater visibility into security threats that target a range of devices while also allowing them to better prioritize their remediation efforts based on the actual likelihood of an attack.

› **The security standards and architecture team writes policies and identifies tools.** Working in conjunction with the enterprise architecture team and various business unit leads, this team determines the specific security policies governing mobile use throughout the digital business ecosystem.[6] For example, strong policies around data discovery and data indexing will help the security team maintain better control over sensitive information on mobile devices.[7] This team can also help implement a Zero Trust approach to mobile security architecture, with better application awareness and data protection to help your security team move toward more device-agnostic, application-centric security.[8]

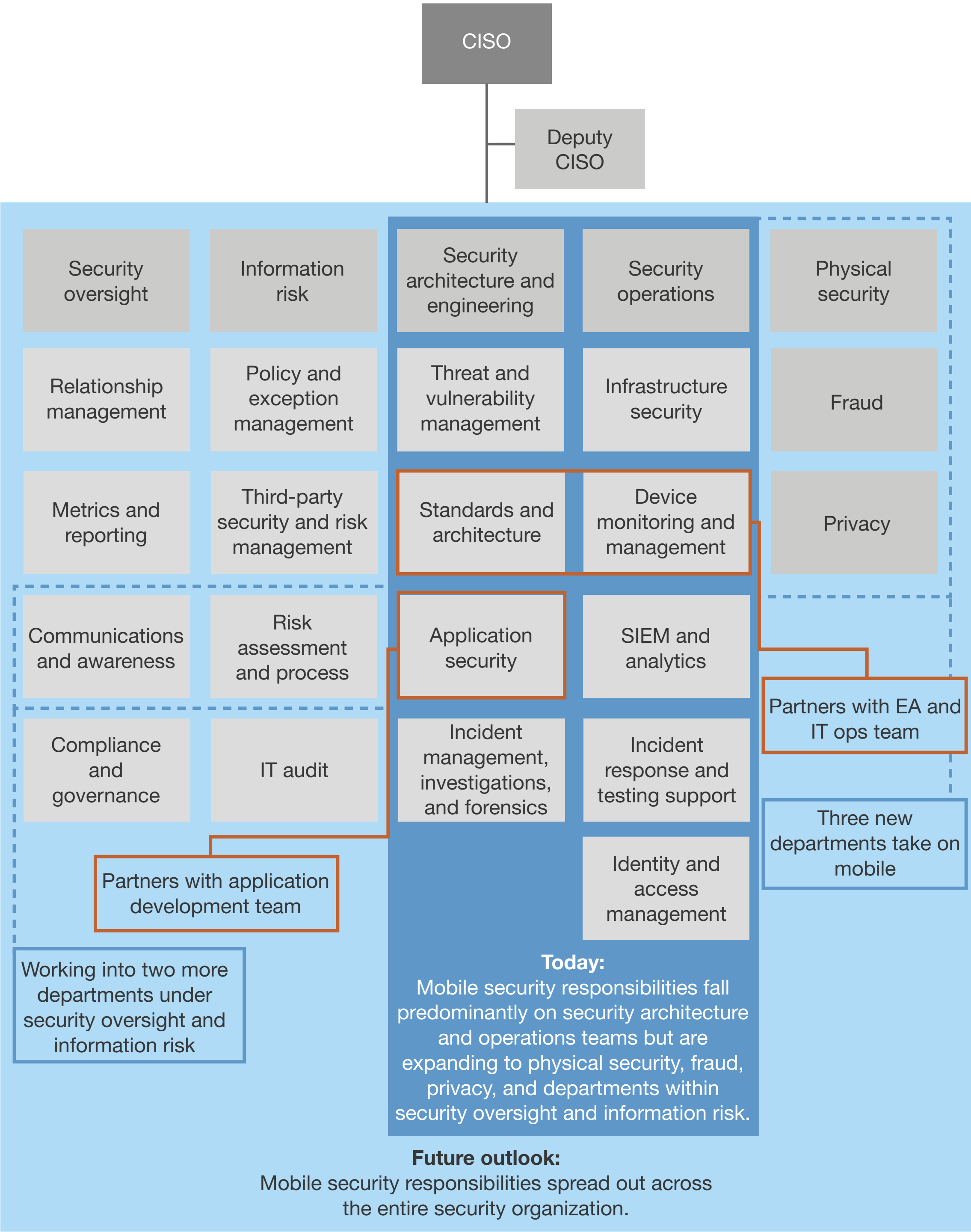
› **The application security team enforces secure mobile application coding practices.** Somewhere in your organization, a developer is building a mobile app right now. To help systematically improve security at the app layer, security pros must join with developers and operations pros in DevOps practices.[9] Working in conjunction with the application development team, application security experts ensure that development teams follow security best practices to reduce the likelihood of app-level vulnerabilities. Mobile application management tools may also be validated here, with the team working alongside the security standards and architecture team to develop the mobile application policy set.

› **Device monitoring and management responds to device-level security events.** Device security staff members investigate alerts raised by IT operations staff members who run tools such as enterprise mobility management (EMM), application-level protection, network-based mobile security gateways, and other (both on-premises and cloud-based) sources of mobile-security-related events and intelligence. Today, many overburdened security teams are offloading their day-to-day mobile security management responsibilities to their IT operations teams; expect this trend to continue as organizations continue to experience a dearth of security talent within the organization.[10]

› **The identity and access management team ensures seamless device integration.** The identity and access management (IAM) team ensures that the organization authenticates these devices properly and controls access to the appropriate back-end data and resources. IAM can also help improve customers' experience using alternative authentication solutions such as biometrics or solutions that are risk-based.[11] Physical security teams are important to include in these IAM strategy discussions as new mobile access technologies flood the market with promise of more secure and smooth access control. This team also monitors changes to permissions and exception requests within the corporate directory and any associated mobile-specific user directories.

› **Privacy and fraud management tighten loose ends.** As privacy concerns become more common for both employees and customers engaging with mobile, it's important that privacy professionals have a hand in your mobile security strategy's core expertise. Privacy is a competitive differentiator, and firms that fail to have a cohesive privacy strategy and program will struggle to succeed at best and be a ticking time bomb for customer outrage at worst. And as commerce shifts to mobile and cybercriminals continue to target mobile for identity theft, fraud management has been forced into the core mobile security strategy conversation. If fraud management gets to the mobile strategy table too late, you can be sure of a significant impact to customer experience and the firm's reputation.[12]

FIGURE 1 Mobile Responsibilities Will Continue To Spread Within And Outside Of Security


CISO
Deputy CISO
Security oversight
Information risk
Security architecture and engineering
Security operations
Physical security
Relationship management
Policy and exception management
Threat and vulnerability management
Infrastructure security
Fraud
Metrics and reporting
Third-party security and risk management
Standards and architecture
Device monitoring and management
Privacy
Communications and awareness
Risk assessment and process
Application security
SIEM and analytics
Partners with EA and IT ops team
Compliance and governance
IT audit
Incident management, investigations, and forensics
Incident response and testing support
Three new departments take on mobile
Partners with application development team
Identity and access management
Working into two more departments under security oversight and information risk

Today:
Mobile security responsibilities fall predominantly on security architecture and operations teams but are expanding to physical security, fraud, privacy, and departments within security oversight and information risk.

Future outlook:
Mobile security responsibilities spread out across the entire security organization.

Increase Security's Alignment With Mobile Business Initiatives

Almost every business unit in your organization is likely either implementing or planning to implement new mobile initiatives. These may include a custom interface that gives traveling sales staff a direct connection to back-end inventory systems or a marketing app that directly engages with customers. Since many of these business innovations will likely occur whether the security team is involved or not, it's up to the security team to come to the table with solutions, especially those that support top-line growth. In fact, our data shows that more business leaders are becoming involved in developing secure customer-facing mobile and web apps than ever before; in 2016, there was a 10 point increase (up from 22% the year prior) of business decision-maker respondents who reported app development was their responsibility.[13]

As mobile initiatives have become more complex and widespread throughout the organization, more formal collaboration between the business units and the mobile project teams is necessary to ensure alignment.[14] There are several ways to accomplish this:

› **Use mobile steering committees to prioritize projects.** In most cases, businesses establish these committees to prioritize mobile initiatives, obtain budget, and set cross-enterprise priorities. Our research confirms that companies well-positioned to succeed had cross-functional mobile steering committees in place.[15] This is a perfect opportunity to reach across the aisle and work with the development and operations team to build a comprehensive mobile strategy across the organization. It's also important to communicate security metrics with senior management, improving mobile security funding opportunities.

› **Engage mobile centers of excellence to provide mobile security thought leadership.** Businesses use mobile centers of excellence to determine and set best practices as well as to teach others about app development, employee security, app sharing, and collaboration across the organization. This center should focus on ensuring the best experience for customers. With the security experience as a traditional pain point, the S&R pro must be involved from the beginning. Although security professionals don't need to participate full time, laying the groundwork and continued alignment is certainly necessary. These centers also present security professionals with an opportunity to enforce secure mobile customer engagement, reducing the organization's risk of a breach.[16]

› **Participate in mobile IDEA teams to ensure security is a design consideration.** Mobile project teams looking to push their apps beyond the basics are now working across multiple business units using what Forrester calls IDEA teams.[17] Firms staff these teams with between four and 10 cross-functional developers, designers, product management, and program management.[18] In a retail organization, for example, an IDEA team would include eCommerce professionals, select retail store staff, mobile developers, and those within the CIO's organization who control and maintain inventory and pricing. Security professionals should participate at the design level of these mobile teams to bake in a balance of security and a strong customer experience from the start.

Security Pros Require Both Technical And Soft Mobile Skills

While few mobile-security-specific roles exist today outside of application development, many security architecture and operations staff members will need to be generalists with an understanding of both the security and organizational implications imposed by mobile devices and apps. Today, 49% of security decision-makers who indicate unavailability of security employees with the right skills is a challenge for their enterprise firm claim mobile security skills and experience are most needed at their organization.[19]

Technical Skills Are Necessary For Designing And Enforcing Controls

The technical skills a mobile security professional needs will vary based on the maturity and size of the security team. Some individuals will need broad mobile security expertise, while others (such as those sitting on the security architecture and operations teams) will require more in-depth technical knowledge in specific domains such as mobile application security or identity and access management. However, some technical skills are mandatory:

› **Staff must understand current and past OS APIs designed for mobile management.** The ability to support the most popular device and operating system is crucial to any successful mobile strategy. Therefore, the individual playing a key role in device certification and support should have deep expertise in a variety of mobile platforms. At the very least, they must understand the attack surface and the tools and settings provided natively through basic mobile device management (MDM) or EMM software. Since MDM and security are very much intertwined, mobile security professionals should also be versed enough in their organization's mobile management requirements to be able to work side by side with their mobile management team to help ensure that they have proper audit and compliance policies in place.

› **Secure mobile application development and delivery is an absolute requirement.** Mobile applications are quickly becoming the primary way employees access corporate resources. It's also becoming one of the most important channels for customer engagement. At the same time, DevOps methodologies are increasing the pace of application releases. The need to securely develop, distribute, and manage mobile applications is critical today. To help systematically improve security at the app layer, security pros must join with developers and operations pros in DevOps practices.[20] They then must layer additional app protection: Application hardening, application wrapping, application reputation services, mobile static code analysis, and application behavioral monitoring are all important security controls that security teams can use to better protect mobile apps.

› **The ability to architect for the entire digital business ecosystem is also required.** As a result of the new customer engagement models, mobile explosion, and rise of cloud services, a business process in a digital business is rarely, if ever, self-contained within the company's four walls. In today's digital business, successful mobile security professionals must have knowledge of application environments driven by application programming interfaces and the ins and outs of federated identity.

- **The ability to think like an attacker drives proactivity.** Threat modeling is the process of identifying threats and vulnerabilities in a system and looking for ways to exploit them. One CISO commented to Forrester, “I want guys who can think like a hacker and break things.” Mobile threat researchers must be able to shift between offensive and defensive perspectives. How can an attacker take advantage of the solution, and how can the security team design controls that reduce the likelihood of this occurring?

You Need Soft Skills To Increase Visibility And Enable Business Innovation

Many mobile security roles require strong soft skills; the security architect especially must be able to understand the business’ mobile requirements. While some organizations are inclined to split the role in two and have a business analyst who collects the requirements and works with an architect on design, ideally the security architect will have the skills to work directly with the business unit leads. Additionally, as more and more investment shifts from traditional information technology to business technology (technology that helps win, serve, and retain customers), it’s more important mobile security professionals partner with their business stakeholders. This requires several key skills:

- **Strong written and presentation skills are necessary to communicate key issues.** Of the security decision-makers who find the unavailability of security employees with the right skills to be a challenge, 40% list communication skills as among the most needed in their organizations today.[21] Security executives must be able to communicate with all levels of the organization to build relationships and increase visibility.

- **Negotiation, persuasion, and influence skills help build support.** This is particularly true in organizations that don’t have a compliance mandate requiring specific courses of action. Influencing decisions is much more challenging in this scenario and can require significantly more finesse. Equally important is acknowledging that there is no perfect solution; with a risk-based approach, budget and schedule can trump security.

- **Social, receptive, and collaborative attitudes help foster collaboration.** The reality is that mobile initiatives are going to occur with or without the direct involvement of security professionals. One enterprise IT services firm said that it prefers its security staff to have both social and teaching skills to help facilitate cooperation (and understanding) between security and the other business units. With that in mind, the security staff should be open-minded and collaborative when working with other parts of the business (e.g., developers, infrastructure pros); they can use the opportunity to learn but also teach other roles about security and its significance.

What It Means

Mobile Security Professionals Must Meet Current And Future Needs

Security teams will need to expand resources to manage the growing diversity of mobile elements throughout their organizations. As they do, this will require security leaders expose their staff to the demands of the workforce and today's empowered customer. Security teams, stretched thin, will offload day-to-day mobile security responsibilities to operations staff. In the next two to three years we expect that:

- **Security oversight will increasingly play a role as the business adopts mobile services.** Leveraging a third-party security provider for mobile security and management is an attractive option for organizations lacking in-house technical expertise; however, the internal security team will need to be increasingly involved in overseeing these relationships.

- **Information risk pros will become aggressive about mobile data loss prevention.** Today, data security and compliance concerns have companies looking to EMM solutions that either offer or integrate with enterprise file-sync-and-share tools, combined with mobile data loss prevention, to provide more control over access to and use of sensitive data.[22] Whether it's mobile DLP, secure file-sync-and-share tools, biometrics, or broader use of in-flight and at-rest encryption as the tools used to perform this essential data security mature, expect this team to become deeply involved in the far-reaching policies governing mobile data use.

- **Privacy staff will become more involved with mobile initiatives.** Global privacy regulations are expanding and evolving, and the fines are growing. In 2018, the fine for a violation of the EU's GDPR will be 4% of global revenues. Unfortunately, it's all too easy for business leaders and developers to use the rich data generated from mobile devices and applications for better employee and customer service. Considering that the trend in global privacy laws today leans toward increased restrictions, prepare for your organization's privacy staff to play a more involved role in your mobile security for both employees and customers.[23]

Supplemental Material

Survey Methodology

Forrester's Global Business Technographics® Security Survey, 2016, was fielded in March to May 2016. This online survey included 3,588 respondents in Australia, Brazil, Canada, China, France, Germany, India, New Zealand, the UK, and the US from companies with two or more employees.

Forrester's Global Business Technographics Telecommunications And Mobility Workforce Survey, 2016, was fielded between October and December 2015. This online survey included 7,342 respondents in Australia, Brazil, Canada, China, France, Germany, India, New Zealand, the UK, and the US from companies with two or more employees.

Forrester's Business Technographics ensures that the final survey population only includes information workers who use a connected device for work at least 1 hour per day. Research Now fielded this survey on behalf of Forrester. Survey respondent incentives include points redeemable for gift certificates.

Please note that the brand questions included in this survey should not be used to measure market share. The purpose of Forrester's Business Technographics brand questions is to show usage of a brand by a specific target audience at one point in time.

Endnotes

[1] Source: Forrester's Global Business Technographics Security Survey, 2016.

[2] For more information, see the Forrester report "Improve Skills And Staffing For A Better Employee Tech Experience."

[3] Source: Forrester's Global Business Technographics Security Survey, 2016.

[4] Source: Forrester's Global Business Technographics Telecommunications And Mobility Workforce Survey, 2016.

[5] For more information on vendors offering unified policy solutions, see the Forrester report "Endpoint Security Suite Market Update: Q2 2013."

[6] See the Forrester report "The Digital Business Imperative."

[7] Data is the lifeblood of today's digital businesses. Protecting it from theft, misuse, and abuse is the top responsibility of every S&R leader. Hacked customer data can erase millions in profits, stolen intellectual property can erase competitive advantage, and unnecessary privacy abuses can bring unwanted scrutiny and fines from regulators while inflicting reputational damage. For more information, see the Forrester report "The Future Of Data Security And Privacy: Growth And Competitive Differentiation."

[8] Forrester's Zero Trust Model of information security banishes the old security motto of "trust but verify" and replaces it with a new motto: "Verify but never trust." When you're trying to protect your organization's intellectual property and sensitive customer data, implicit trust assumptions are dangerous because they leave your organization vulnerable to so-called "trusted insiders" and become obsolete when the environment or technology changes — and in a world defined by continued digital disruption, your environment and your technology are always changing. The following report provides security and risk professionals with an overview of how security architectures and operations are evolving to support today's digital businesses and implementing the core concepts and tenets of the Zero Trust Model. For more information, see the Forrester report "Transform Your Security Architecture And Operations For The Zero Trust Ecosystem."

[9] See the Forrester report "Secure Applications At The Speed Of DevOps" and see the Forrester report "How To Differentiate With Excellent Mobile Customer Service."

[10] For more information on hosted security services and endpoint trends, see the Forrester report "The State Of Endpoint Security Adoption 2014 To 2015."

[11] For more information on alternative authentication solutions, see the Forrester report "How To Get Away With Murder: Authentication Technologies That Will Help You Kill Passwords."

[12] Data is the lifeblood of today's digital businesses; protecting it from theft, misuse, and abuse is the top responsibility of every S&R leader. Hacked customer data can erase millions in profits, stolen IP can destroy competitive advantage, and unnecessary privacy abuses can bring unwanted scrutiny and fines from regulators while damaging reputations. S&R pros must take a data-centric approach that ensures security travels with the data regardless of user population, location, or even hosting model; position data security and privacy capabilities as competitive differentiators; and build a new kind of customer relationship. For more information, see the Forrester report "The Future Of Data Security And Privacy: Growth And Competitive Differentiation."

[13] Source: Forrester's Global Business Technographics Security Survey, 2016.

[14] See the Forrester report "Organize For Mobile Success."

[15] See the Forrester report “Organize For Mobile Success.”

[16] For more information on the importance of being customer-obsessed, see the Forrester report “Technology Management In The Age Of The Customer.”

[17] See the Forrester report “Organize For Mobile Success.”

For more information on Forrester’s IDEA framework, see the Forrester report “Mobile Moments Transform Customer Experience” and see the Forrester report “Re-Engineer Your Business For Mobile Moments.”

[18] For detailed views of how these IDEA teams should be structured, see the Forrester report “Organize For Mobile Development Success.”

[19] Source: Forrester’s Global Business Technographics Security Survey, 2016.

[20] See the Forrester report “Secure Applications At The Speed Of DevOps” and see the Forrester report “How To Differentiate With Excellent Mobile Customer Service.”

[21] Source: Forrester’s Global Business Technographics Security Survey, 2015.

[22] For more information on data loss prevention and key components of enterprise mobile management solutions, see the Forrester report “Market Update: Security Remains A Key Component To Enterprise Mobile Management.”

[23] For more information on data privacy and global privacy laws, see the Forrester report “Q&A: EU Privacy Regulations” and see the Forrester report “Forrester’s 2016 Interactive Data Privacy Heat Map.”

FORRESTER®

CHALLENGE THINKING. LEAD CHANGE.

We work with business and technology leaders to develop customer-obsessed strategies that drive growth.

PRODUCTS AND SERVICES

- Core research and tools
- Data and analytics
- Peer collaboration
- Analyst engagement
- Consulting
- Events

Forrester's research and insights are tailored to your role and critical business initiatives.

ROLES WE SERVE

Marketing & Strategy Professionals

CMO

B2B Marketing

B2C Marketing

Customer Experience

Customer Insights

eBusiness & Channel Strategy

Technology Management Professionals

CIO

Application Development & Delivery

Enterprise Architecture

Infrastructure & Operations

› Security & Risk

Sourcing & Vendor Management

Technology Industry Professionals

Analyst Relations

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 Research (Nasdaq: FORR) is one of the most influential research and advisory firms in the world. We work with business and technology leaders to develop customer-obsessed strategies that drive growth. Through proprietary research, data, custom consulting, exclusive executive peer groups, and events, the Forrester experience is about a singular and powerful purpose: to challenge the thinking of our clients to help them lead change in their organizations. For more information, visit forrester.com. 110761