Healthcare Edition

5th Annual State of Application Security Report

Perception vs. Reality

January 2016

ARXAN

Table of Contents

Executive Summary

More than half (55%) of consumers who use mobile health applications expect their health apps to be hacked within the next six months. So too do nearly half of executive IT decision makers (48%) who have oversight or insight into the security of the mobile healthcare apps they produce. This sentiment makes it sound like mobile health applications are at a hopeless state of security where, despite Herculean efforts to thwart attackers, adversaries are expected to prevail. But it's not hopeless. It's careless. Especially when you consider that 50% of organizations have zero budget allocated for mobile app security[1].

It is crucial for organizations with mobile health apps to double-down on app security. Why? If they don't, they risk losing customers.

76% of health app users indicated they would change providers if they knew the apps they were using were not secure. And 80% of health app users would change providers if they knew alternative apps offered by similar service providers were more secure. While millennials are driving the adoption of mobile apps, their views on the importance of app security were equally as strong as the older non-millennials. In general, survey results showed very little geographical discrepancies across the US, UK, Germany, and Japan. Interestingly, however, while the iOS operating system is often viewed as more secure than Android, iOS apps were shown to be more vulnerable than Android apps in this study.

Executive Summary (cont'd.)

So should we expect a critical mass of consumers to walk away from organizations because their mobile health apps do not have the level of security protection they expect? Based on these research findings, perhaps. When put to the test, the majority of mobile health apps failed security tests and could easily be hacked. Among 71 popular mobile health apps tested for security vulnerabilities, 86% were shown to have at least two OWASP Mobile Top 10 Risks[2]. Such vulnerabilities could allow the apps to be tampered and reverse-engineered, put sensitive health information in the wrong hands and, even worse, potentially force critical health apps to malfunction. Surprisingly, US Food and Drug Administration (FDA)-approved apps and formerly UK National Health Service (NHS)-approved apps were among the vulnerable mobile health apps tested, indicating that there is more work to be done by governing bodies to better understand the cybersecurity threats to mobile apps and improve the minimum acceptable security standards or regulations for mobile app development.

Mobile app security is becoming an increasingly important decision-making factor for consumers seeking to do business with organizations they can trust to protect their privacy and provide robust security. For organizations with mobile health apps, this means that security can be used as a competitive differentiator to help attract and retain app users and patients.

While it's clear *why* organizations should mitigate the security, safety, financial, and brand risks associated with vulnerable mobile apps, it's less clear what organizations and consumers should do to improve protection. This report provides recommendations for how organizations and consumers can minimize the risk of their mobile apps being hacked.

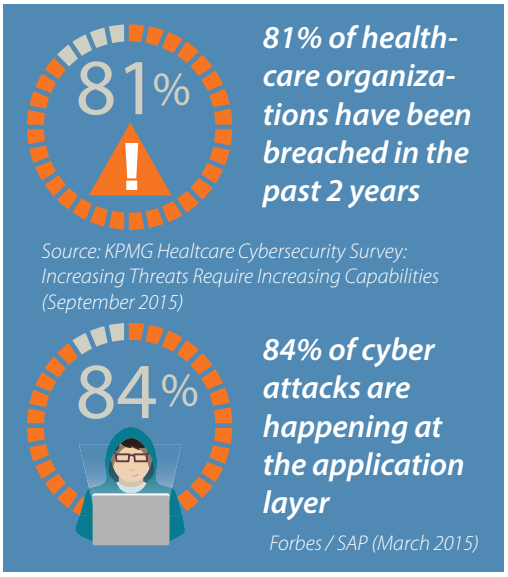
Methodology

Arxan commissioned a third-party, independent research organization in November 2015 to undertake an electronic survey of 1,083 individuals in the US, UK, Germany, and Japan:

- 815 consumers who use mobile health and mobile finance apps
- 268 IT decision makers within organizations that produce mobile health and mobile finance apps and who also have oversight or insights into the security of those mobile apps

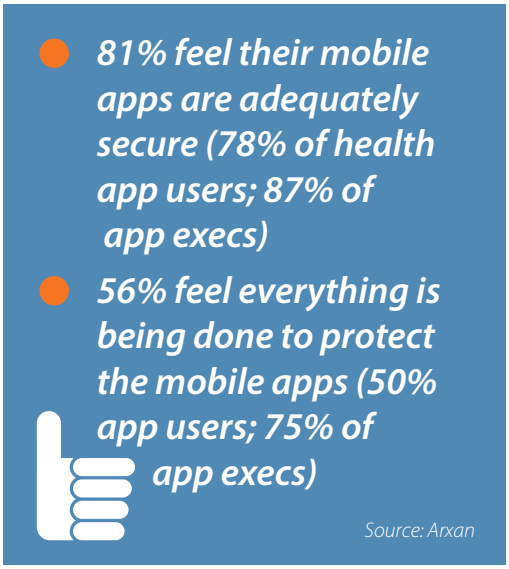
Also in October and November 2015, a third-party independent analysis of a total of 71 popular mobile health apps from each of the four countries was undertaken leveraging Mi3 Security solutions. Arxan selected the apps from among the most popular mobile health apps for the Android and iOS platforms for each region. Included among the apps tested were 19 mobile health apps approved by the US Food and Drug Administration (FDA) and 15 mobile health apps that were previously approved by the UK National Health Service (NHS).[3]

The Findings



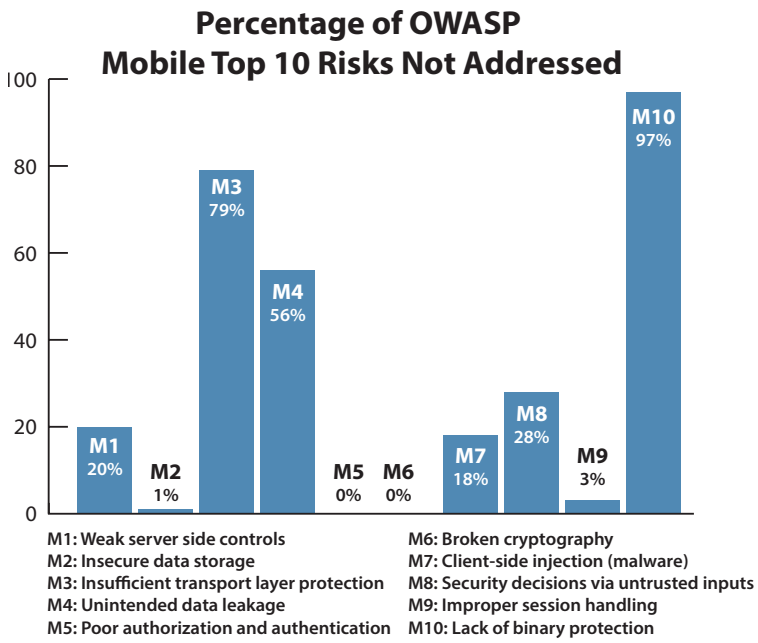
Healthcare organizations are among the top targets of hackers in search of valuable patient/health data and intellectual property.

It's not all that surprising given that a complete medical record can fetch upwards of $500 in the underground market[4]. Equally unsurprising is that the majority of healthcare organizations have already been breached. Given that the vast majority of cyber-attacks are happening at the application layer, one would think that robust application security would be a fundamental security measure being taken and increasingly required by regulators, particularly given the healthcare community's rapid advancement toward mobile and IoT.



Folks *think* their mobile health apps are adequately secure.

Users of mobile health apps and IT decision makers with insights into the security of mobile health apps feel that their mobile apps are adequately secure. In fact, most feel that app developers are doing everything they can to protect their health apps.

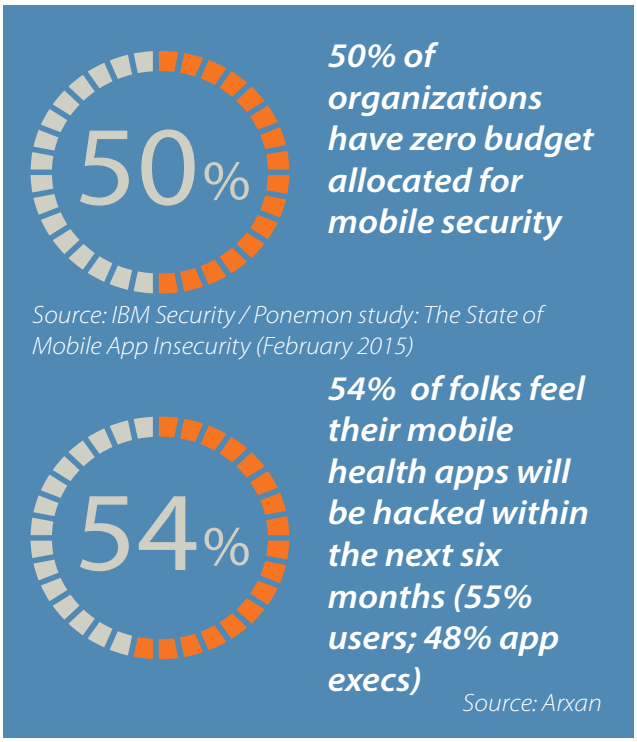


Think again.

Perception is not reality. Most health apps have significant vulnerabilities. Vulnerability assessments were conducted on 71 mobile health apps in the US, UK, Germany, and Japan. The vulnerability assessments were based on the Open Web Application Security Project (OWASP) Top 10 Mobile Risks[5].

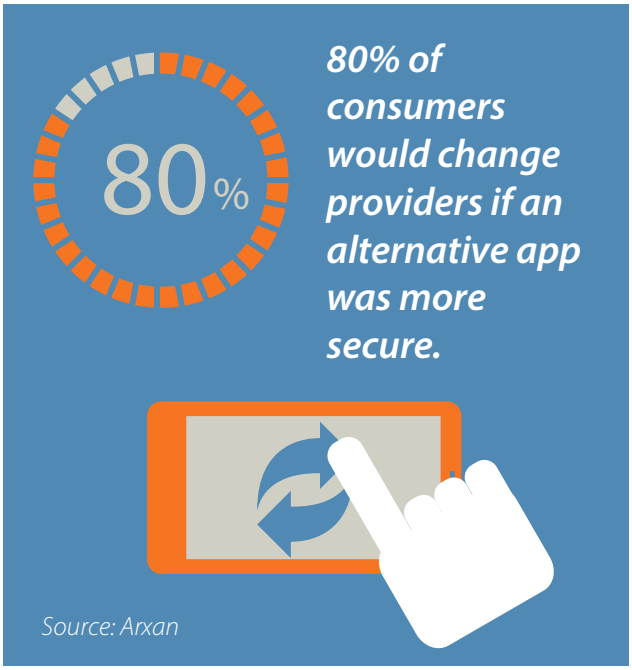
Included among the health apps tested were a sample of health apps approved by the US Food and Drug Administration (FDA) and apps formerly approved by the UK National Health Service (NHS)[6]. Interestingly, 84% of the FDA-approved apps that were tested were not adequately addressing at least two of the OWASP Mobile Top 10 Risks. Similarly, 80% of the apps formerly approved by the NHS that were tested were not addressing at least two OWASP Mobile Top 10 Risks.

According to Arxan CTO Sam Rehman, "The impact for healthcare organizations and health app users can be devastating. Imagine having your mobile health app leak your personal health information or your app reprogrammed to instruct you to deliver a lethal dose of medication."



Shocking? Not really.

Many companies are not investing in mobile app security. According to IBM Security and Ponemon research[7], 50% of organizations allocate no budget for mobile app security. Perhaps this is why more than half of all respondents feel that their apps are likely to be hacked within the next six months.



Who cares? You do.

Even without experiencing a cyber-attack on their app, about 80% of health app users would change providers if their app is known to be vulnerable or if an alternative app is more secure. Interestingly, more than 75% of mobile health app executives also believe that users would change providers if they knew their apps were insecure or if a similar provider offered a more secure mobile app.

Ignorance *must* be bliss.

There were more than three billion mHealth apps downloaded in 2015 from major app stores[8]. And if health app users actually knew how vulnerable their apps really were, according to this study, we should expect a mass exodus of users fleeing to healthcare organizations that develop more secure, trusted mobile apps.

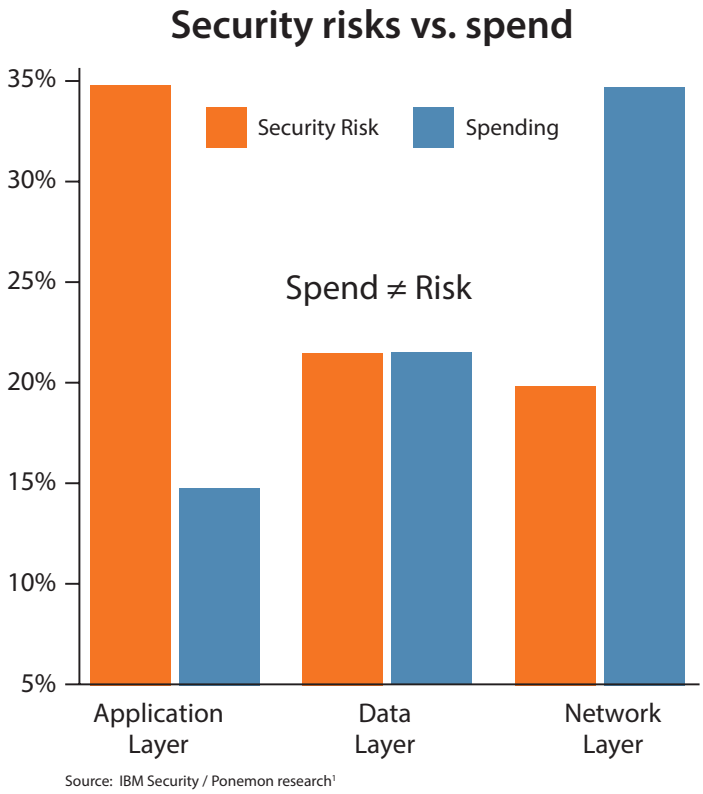
Recommendations

What can be done?

For healthcare organizations:

- ***"Set your security bar above the regulations"*** Regulatory bodies lag beind cyber criminals and likely always will. Apps "approved" by trusted sources such as regulatory / governing bodies like the US Food and Drug Administration (FDA) or those formerly approved by the UK National Health Service (NHS) are no more secure than unapproved apps.

- ***Strengthen the weakest links.*** Address elements of the OWASP Mobile Top 10 Risks that are being neglected. 79% of the apps tested had a transport layer vulnerability. 97% of the health apps tested lacked binary code protection – the most prevalent security vulnerability identified.



Source: IBM Security / Ponemon research[1]

- ***Make security a source of competitive advantage.*** Market the strength of security you offer to attract and retain patients and health app users.

- ***Align spending with risks:*** IBM Security and Ponemon research[9] reveals that the majority of risks are happening at the application layer, but the spending is largely focused on networks and data.

For consumers:

- ***Get apps only from authorized app stores.*** Most authorized app stores have some security protocols in place to help ensure apps can be trusted.

- ***Don't jailbreak or root mobile devices.*** Jailbreaking/rooting devices negates security measures that are designed to help protect you and your data.

- ***Demand more transparency about the security of the apps you are using.***
  As cliché as it is, knowledge is power – many foods you eat are usually required to be labeled with nutrition information to help you make better-informed decisions. Before you download a mobile app, wouldn't you want to know what risks you may be opening yourself up to? Become an advocate for app security certification and risk transparency.

For policymakers and regulators:

- ***Establish a "Good Housekeeping" seal of approval for app security.*** Require apps to make available an OWASP Mobile Top 10 Risk rating for critical apps. Consumers need to know what risks they are accepting before downloading or "consuming" an app. And the healthcare community, including healthcare providers, medical device manufacturers, and others need to incorporate risk as a fundamental consideration before making app recommendations to patients and app users.

Learn More

- View and share the infographic: https://www.arxan.com/resources/state-of-application-security/
- Download a Mobile App Security Handbook: https://www.arxan.com/resources/mobile-application-protection-handbook/

Contact Us

Stephen McCarney
Arxan Technologies
Tel: +1 301-968-4295
Email: smccarney@arxan.com

Footnotes

[1] IBM Security / Ponemon study: *The State of Mobile Application Insecurity* (February 2015)
[2] The Open Web Application Security Project identifies the most critical application security risks facing organizations
[3] The UK NHS Health Apps Library included 79 apps, which were approved by the NHS. The NHS library of approved apps closed in October 2015 after Arxan had tested a sample of 15 NHS-approved apps.
[4] NPR: *The Black Market for Stolen Health Care Data* (February 2015)
[5] *Ibid.* [2]
[6] *Ibid.* [3]
[7] *Ibid.* [1]
[8] *mHealth App Developer Economics 2015*
[9] *Ibid.* [1]