Perceptions of Risk in Mobile Transactions

Shari Trewin, Cal Swart, Larry Koved, Kapil Singh
IBM T.J. Watson Research Center
P.O. Box 218
Yorktown Heights, N.Y. 10570
trewin@us.ibm.com, cals@us.ibm.com, koved@us.ibm.com, kapil@us.ibm.com

***Abstract*— Mobile users are unlikely to guard against information security risks that do not come to mind in typical situations. As more people conduct sensitive transactions through mobile devices, what risks do they perceive? To inform the design of mobile applications we present a user study of perceived risk for information technology workers accessing company data; consumers using mobile personal banking; and doctors accessing medical records. Shoulder surfing and network snooping were the most commonly cited classes of risk, and perceived risk was influenced by the surrounding environment and source of information. However, overall risk awareness was low. The possible risks of device theft and loss, hacking, malware and data stored on devices were not prominent concerns. The study also revealed differences in the way the groups think about network-related threats. Based on these results, we suggest research directions for effective protection of sensitive data in mobile environments.**

Keywords- Risk perception, Smartphones, user study.

I. INTRODUCTION

When people perform sensitive transactions on mobile devices, security is just one of many factors the user is balancing. A doctor may need instant access to medical test results, or a businesswoman may have million dollar deals awaiting her decisions. Unless the user is a security professional, risks such as phishing attacks, network sniffing, untrustworthy WiFi networks, malware on their devices, phone-snatching thieves, or casual shoulder-surfers, are not their primary focus.

On the other hand, for organizations providing sensitive information such as medical or corporate data to authorized users on mobile devices, security is a critical component of their solution, and these threats are very real. Rather than blaming users for resisting or undermining security measures, it is nowadays recognized that usability is an essential component of security, and that the user's perspective and broader set of concerns need to be considered when designing security solutions, or assessing risks. With this in mind, it is important to understand the user's perception of risks, and how it differs from the organization's perspective.

The aim of this paper is to contribute to our understanding of perceived information security risks in sensitive mobile transactions. We present an empirical study covering three distinct user scenarios: technology company workers accessing company information, people accessing personal financial information, and doctors accessing medical records.

We compare users' perceptions with the risks perceived by a group of security experts, representing the set of possible risks an organization may need to protect against. We refer to these as the "possible risks". Our primary findings are:

- The surrounding environment of the user significantly impacts perceived risk, with the two most important factors being trust in the safety of network communications, and shoulder surfing risk. Home and office environments (and networks) are trusted. Some public environments are trusted when shoulder surfing risk is minimal.
- Trusted web sites and trusted apps are both perceived as safe to use for sensitive transactions on a smartphone. Phishing may therefore be a significant threat on mobile devices, where traditional security indicators are not typically provided. Users may need greater awareness of the risks through improved communication of security risks.
- Possible risks that do not come readily to the minds of users when deciding to perform a sensitive transaction include device theft and loss, malware, device hacking and cloud/device storage of data. Organizations should take this lack of concern into account in the design of organizational security requirements.
- In-network risks were mentioned by approximately half of the participants. However, the corresponding actions and assessment vary considerably based on the user group. As an example, we found that IT Workers (like IT Security Experts) focus on VPN protection of network traffic. Personal Banking Consumers are 50% less likely to specifically mention VPN or encryption. Doctors accessing medical records wanted reassurance that the network connection could be trusted, and relied on the security standards implemented in their medical app.
- Even when users are aware of risk, other factors such as need for the information may override any security concerns. Where users are knowingly choosing to take a risk, this is fertile ground for usable mobile security research.

This paper presents findings from three user groups, followed by a discussion of the differences between groups, and the implications and limitations of this work.

DOI 10.1109/SPW.2016.37

II. RELATED WORK

The risks of performing a sensitive transaction on a mobile device in a specific environment will change over time. In 2012, smartphone theft reportedly accounted for 30-40% of all crime in major cities in the United States [12], and in 2013 annual smartphone theft almost doubled, to 3.1 million [7]. The Lookout mobile security company estimates that the average American consumer loses their cellphone once every year [27], with coffee shops and bars being the most common places phones are lost or stolen [27]. 90% of people picking up lost smartphones will try to access sensitive data [33]. There is evidence that mobile phones are also at risk of unauthorized access by insiders [28].

A survey of commuters found that 66% in Europe and 72% in the UK do look at what their fellow commuters are doing on their devices, often seeing confidential or sensitive information [11]. However, a month-long field study of smartphone users found that only 0.3% of sampled mobile access situations posed a potential shoulder surfing risk [17].

A. Risk Perception

Non-experts assess risk very differently than experts [19]. While experts use statistical reasoning, non-experts do not assess risk in a logical, consistent way [4][10][35]. They often rely on affect [10], and are unduly influenced by the perceived degree of damage that will be caused.

Furthermore, people's risk assessments are also influenced by their ability to imagine the outcome, their exposure to examples of such outcomes, and their personal experience of taking similar risks in the past [4]. In a focus group, Huang et al [17] found that participants saw the risk of their phone being lost or stolen as being highly controllable and unlikely to happen.

Factors that have been shown to influence perception of risk in information security include familiarity with the risk, degree of dread associated with the risk, ability to choose whether to take the risk, immediacy of effect, and severity of the consequences [14][16]. Online risks that can be easily related to known risks in the physical world are better understood and considered more serious [14]. This implies that people may be more aware of device loss and theft than of invisible, network-related threats. Indeed, studies of home network [37] and WiFi users [23] have found that non-experts may have a false sense of security and do not fully protect themselves. While this could be attributed to lack of knowledge, Herley [15] points out that much security advice offers little benefit for the investment required in acting on it, and users' decisions to ignore such advice are often rational when viewed in economic terms.

Although perceived risk for online financial transactions is higher than for social networking [26], Davinson and Sillence [8] found low perceived threat levels for online bank transactions, due to participants' thinking it unlikely that they would be a victim of fraud, and not feeling responsible for any negative outcomes. Huang et al. [17] found that people who have a high level of knowledge of the risks, and perceive them as controllable and easy to detect, are more likely to adopt an online banking solution. This suggests that providing such knowledge to users could potentially increase adoption of mobile solutions.

Chin, Felt, Sekar and Wagner [7] surveyed smartphone users about their willingness to perform potentially sensitive activities on their phone and their laptop, finding that 60% of respondents would not enter a social security number on their phone due to security concerns, while only 7% had such concerns on a laptop. When asked about online banking, 13% of respondents would not do this on their phone for security reasons, with their concerns being that the phone may be hacked into or lost. Participants cited several sources of security concern for smartphones: Wi-Fi and 3G networks, lack of anti-virus software, ease of losing phones, and lack of knowledge about phone security. The paper does not report the frequency with which these factors were mentioned. Participants also had some misconceptions about security. For example, some participants concerned about WiFi phone connections did not have similar worries about the same connections when used with a laptop. Furthermore, some participants were suspicious of cellular connections because no password was needed. After discussing security concerns, participants were also asked a general question about worries and fears in using a smartphone. 28% cited the possibility of losing it, or it being stolen, and the information lost was an important factor in this concern.

B. Security Measures and Communicating Risk

The risks associated with smartphone loss or theft can be reduced by activating the device's lock feature. A 2011 survey by Confident Technologies [6] found that only 47.1% of 126 respondents used a password or PIN to lock their smartphone or tablet. 44% of those who did not lock their devices found the password too cumbersome, while 30% were not worried about the risk. The remaining 25% 'just never thought about it'.

Uffen, Kaemmerer and Breitner [36] explored the aspects of personality that determine a smartphone user's intentions to use security measures such as device locking or remote wipe. Key determinants were their beliefs about the usefulness of the measures, and whether they feel that use is under their control.

In a traditional desktop / browser setting, there have been numerous studies on phishing (e.g., [16] [31]) and security warnings (e.g., [2][16][24][32]). The challenge has been to provide appropriate warnings that are noticed and acted upon by the user. Many people do not pay attention to online security warnings [21]. In one eyetracking study, Kirlappos, Sasse and Harvey [22] found that 38% of participants did not look at trust seals on websites when evaluating their trustworthiness. Although trust seals did increase trustworthiness ratings when they were noticed, participants often had inaccurate heuristics for assessing risk.

In the mobile computing context, communication is constrained by the device display size and many differences in how the web browsers implement (or fail to implement) risk communication. Some of the security indicators that were previously available are no longer present in mobile devices - for example, visibility of "https" in the url, see [1] for a survey.

Keith, Thompson, Hale, Lowry and Greer [20] studied location and personal information sharing behavior of a large (over 1000 people) group of people who believed they were testing an app that shared location-based messages. Risk information provided to participants did impact their perception of privacy risk, and this risk perception related to their actual practice more strongly than their stated behavioral intentions did.

Tversky and Kahneman observe *"the risk involved in an undertaking may be grossly underestimated if some possible dangers are either difficult to conceive of, or simply do not come to mind."* [34]

The studies above did not explore what risks come naturally to mind for device users in mobile contexts. Knowing these risks would aid in our understanding of user perceptions of risk for mobile transactions, which in turn will inform the design of appropriate security mechanisms and risk communication. Our studies aim to contribute to such an understanding.

III. Study of Risk Perception

A. Participants

We selected groups and scenarios that represent different sensitive transactions that could be performed on mobile devices, covering employees, consumers and medical providers. We expect a more sensitive transaction to elicit more security concerns. Bring-your-own-device (BYOD) concerns are prominent for enterprises. Corporations are moving to provide employees with mobile access to information needed for their job roles, including confidential information. Personal banking information is accessible from mobile devices. Medicine is moving to mobile devices for rapid access to records and test results from anywhere. These types of data differ in the kind of damage caused by a leak, and who is liable. Thus they may elicit different perceived risks. We obtained ethical approval and informed consent for all groups.

B. Information Technology Workers (IT Workers)

The IT Workers were 53 employees of a large information technology corporation, all of whom had owned a smartphone for at least 6 months. Reflecting the gender imbalance in this workplace, 46 of the respondents were male. They were aged between 23 and 67, with a mean age of 44.7 years (Std Dev. = 12.4). Seven respondents declined to give their age. Their self-reported security expertise was: 1=minimal, 26=average, 24=knowledgeable and 2=expert.

34 participants owned an iPhone, 17 owned an Android phone (2 owned both iPhone and Android), 2 owned a Blackberry phone, and 2 had another type of phone.

C. Consumers Using Mobile Personal Banking (Personal Banking)

76 people were recruited from the Amazon Mechanical Turk online marketplace (www.mturk.com). We report here only the responses from the 54 respondents (38 male) who met all inclusion criteria, including owning a smartphone for at least 6 months. Most (27) were aged 20-29, 12 were 30-39, 11 were 40-49, 4 were over 50, and 2 were 18-20. Their self-reported IT security expertise was: 5=minimal, 31=average, 16=knowledgeable and 2=expert.

In contrast to the IT Workers, most participants (34) owned an Android phone, 20 owned an iPhone, 2 owned a Blackberry and 1 owned another type of smartphone. More information about the demographics of Mechanical Turk workers can be found in [30].

D. Doctors

We surveyed 11 doctors (9 male, 2 female) working in a variety of specializations. All had some kind of iOS device (phone or tablet). 8 had an iPhone, 2 had an Android phone. 5 had an iPad.

All reported a need for immediate access to medical information while they are away from their practice or hospital. Two reported using an iPad or an iPhone for access.

E. Materials

We developed a questionnaire, in which a security risk was defined as *"the risk of someone else getting unauthorized access to the information you are viewing or providing"*.

Initial questions covered phone ownership and current phone locking method. Respondents were then given a specific mobile app information access scenario and asked about places and times where they would expect to use the app. Each user group was given a different, appropriate scenario: an app for accessing internal company systems for the IT Workers (CompanyApp), a mobile banking app for the Personal Banking Consumers (BankApp), and an app for accessing medical records for the Doctors (MedicalApp).

The questionnaire then presented a set of six environments. Continuing with the CompanyApp, BankApp and MedicalApp scenarios, participants were asked: *"Imagine yourself in the following places. You need to <do task>. Would the information be safe if you did that in these places?"* The tasks were:

- *"use <company>'s application to look up something about an unannounced acquisition"* (IT Workers);
- *"use the bank's app to look up your account balance"* (Personal Banking); and
- *"use the app to look up something about a patient's health record"* (Doctors)

The environments were the same in all studies, and included a variety of high and low risk situations: familiar and unfamiliar places, different kinds of likely connection method, and different risks of theft or observation. They were described as:

- **At home by yourself**, a low risk, familiar environment with the user's own network and no risk of theft or direct observation.
- **In a crowded local street**, a high risk, familiar environment with cellular network connection and assumed higher risk of theft or direct observation.
- **On a quiet train at night with no-one nearby**, a medium risk, relatively familiar environment with cellular network connection or operator-provided

network connectivity, and no risk of theft or direct observation.

- **In your office at your desk**, a low risk, familiar environment with company-provided network connectivity and assumed low risk of theft or direct observation.
- **In a very busy café in an unfamiliar neighborhood**, a high risk, unfamiliar environment, usually with café-provided network connectivity and assumed high risk of theft or direct observation.
- **In a Beijing hotel room**, a high risk, unfamiliar environment with hotel-provided network connectivity, and no risk of theft or direct observation.

At the time of the survey, there had been recent press stories about hacking activities allegedly originating in China. The intent of using a Beijing hotel room was to evoke an image of a foreign / unfamiliar environment with higher security risk.

Responses were given on a 5-point scale ranging from 'not safe' to 'safe'.

The next questions asked about the appropriate level of authentication for the transaction (not reported here), and then IT Workers and Personal Banking groups were presented with two further scenarios, each with the same six environments. One was identical to the first scenario, but involved a web site instead of an app (TrustedWeb, BankWeb), and the other involved using a credit card on the web site of an unknown online retailer (UnknownRetailer1/2)

Three open questions followed the scenario(s):

- What Else: *"What else would you want to know about the situations described in this study to decide whether it is safe to access or enter sensitive information on your smartphone there?"* Responses to this question reveal factors that the individual would consider when evaluating risk.
- Security Risks: *"What, if any, are the security risks you see in these situations?"* Responses here indicate the specific threats that the individuals are aware of.
- Decision Factors: *"What factors affect your decision whether to access sensitive information in a given situation?"* This question goes beyond risk perception to reveal other factors that people will take into account when deciding whether to accept the perceived risk.

To inform the selection of environments in future studies, Personal Banking consumers were also asked whether there were other places they go where they would be worried about accessing sensitive data on their smartphone.

Finally, the questionnaire requested demographic information covering gender, age and self-reported level of security expertise.

As a check to ensure that Personal Banking participants had read and understood the scenario, and to allow identification of poor quality responses, a comprehension question was inserted after each scenario had been presented for this group only. These questions could be answered by repeating information provided in the scenario. For example, "What does the bank's app comply with?" Initial instructions to Personal Banking participants indicated that a $1.00 bonus would be paid if the comprehension questions were answered correctly and detailed answers were provided for the written responses.

IV. PROCEDURE

A. IT Workers

The questionnaire was distributed on paper and as a Web form within the organization, among employees not specializing in security. Anyone who had owned a smartphone for at least 6 months was eligible to participate. The questionnaire was distributed shortly after most employees had completed their annual certification of business conduct guidelines, including their responsibilities to protect the company's information. The questionnaire was completely anonymous. No compensation was given for completing the questionnaire. It took 10-20 minutes.

B. Personal Banking

The Amazon Mechanical Turk crowdsourcing site was used to distribute the questionnaire to potential personal banking consumers. In this recruitment method, it is necessary to take steps to identify participants who will perform the task with attention and honesty [9], so for quality control, the questionnaire task was restricted to workers with at least 1000 completed tasks, and at least 95% of those tasks accepted as good quality work. We also restricted the survey to US-based workers, for legal reasons.

Workers were paid $0.50 for completing all questions, with a bonus of $1.00. A pilot test was performed to check presentation and pricing for the task. Analysis was limited to participants who indicated that they had owned a smartphone for more than 6 months (16 of 76 were excluded), and responded correctly to all three of the test questions (6 of the remaining 60 were excluded).

C. Doctors

The questionnaire was distributed on paper in a hospital where the doctors were affiliated, during a visit from our researchers. Two doctors filled in the same questionnaire by email. Doctors were given a $50 gift voucher by the hospital for their participation.

D. Analysis

To generate a reference point against which to compare participant responses, we consulted 11 security experts working in the same large technology company as the IT Workers (all male). Ten had over 10 years' IT security research experience and one had 5 years' experience. Through consensus in a group discussion using the same materials as the IT Workers, these experts generated a set of possible risks, representing the risks an organization security department may perceive.

Statistical analysis used non-parametric statistics to assess perceived risk because they provide better reliability than parametric methods on a 5-point response scale. For multiple group comparisons, Kruskal-Wallis H tests were used. Mann-Whitney U tests were used for pairwise

comparisons. Security Expert responses are not included in the statistical analysis.

The three open questions (*'what else', 'security risks',* and *'decision factors'*) were analyzed by post-coding all responses from all three studies. For each question, the procedure was as follows:

1. Each person's response was split into separate comments based on line breaks, sentence breaks, and use of lists.
2. A set of codes was derived by starting from the possible risks given by the Security Experts, and adding or subdividing codes as necessary to cover themes emerging from the data.
3. A coding sheet was prepared and then two different coders applied the codes to the data independently.
4. Differences in code assignment were reviewed and the codes revised and independently re-applied by each coder.
5. After the independent coding, an inter-rater reliability analysis using the Kappa statistic was performed to determine consistency between the coders.

A Kappa statistic greater than 0.8 is considered to indicate an excellent level of agreement between two raters [25]. For our two raters, the Kappa values achieved were:

- *'what else'* question, Kappa = 0.89 ($p<.0.001$);
- *'security risks'* question, Kappa = 0.917 ($p <.0.001$);
- *'what factors'* question, Kappa = 0.879 ($p <.0.001$).

Comments that had been coded inconsistently were discarded, and the codes applied to each person were consolidated, so that no person contributed more than one count to a given code. For the 'what else' question we discarded 18% (47 out of 258 comments). For the 'security risks' question we discarded 8% (24 out of 297 separate comments). For the 'what factors' question we discarded 11% (30 of 261 separate comments).

E. Results

1) Phone Lock

Overall, 46% of the participants did not lock their phones. Those who did use a lock predominantly used the iPhone's 4-digit PIN code, while others used the Android gesture-based unlock. Some IT workers (13%, 7 people) used an 8-character corporate-compliant password on their phones, as required by the company to enable VPN access to company information from the phone. Use of phone locking was higher among the IT Workers, where 68% used a lock on their smartphone (64% when those with company passwords are excluded), compared to 41% among personal banking consumers and 55% among doctors.

2) Perceived Information Safety

Environment has a significant effect on perceived safety when using a trusted app. We compared responses for different environments using only the first (trusted app) scenario in each group (CompanyApp, BankApp, MedicalApp), finding a significant effect of environment on perceived safety (Kruskal-Wallis Chi-Sq=329, df=5, $p<0.001$). As illustrated in Fig. 1, the home and office environments were highly trusted, the crowded local street, busy café and Beijing hotel room were not trusted by most participants, and the quiet train was intermediate. Significance tests at the 5% level, with Bonferroni corrections ($p<0.0033$), indicate significant differences for all pairwise comparisons ($p<0.001$), with the following exceptions: the street, café and hotel scenarios are not significantly different from each other ($p>=0.152$), and the home and office environments are not significantly different ($p=0.194$).

These responses are in line with those of the Security Experts, who rated the home, office and quiet train environments as 'Probably Safe' (assuming the office is private), the busy café and crowded street as 'Probably Not Safe' or 'Not Safe' (shoulder surfing risk), and the Beijing hotel as 'Not Safe' (perceived high probability of network eavesdropping). Some experts felt that if the application was developed and tested sufficiently well, any hotel room would be safe, no matter where.

Turning now to the perceived safety of specific scenarios, the UnknownRetailer tasks were considered 'Not Safe' or 'Probably Not Safe' by 43% of IT Workers and 49% of Personal Banking participants, compared to 34% or less for other tasks. Security Experts also considered the UnknownRetailer1 scenario 'Not Safe', regardless of environment.

Separate analysis of the IT Worker and Personal Banking data sets indicated that in both cases there was a significant overall effect of task on perceived safety (IT Workers: Kruskal-Wallis Chi-Square=39, $p<0.001$; Personal Banking: K-W Chi-Square=53, $p<0.001$). In the IT Worker group, pairwise comparisons (Mann-Whitney with Bonferroni corrections, 5% significance at $p<0.017$) indicated that the CompanyApp and CompanyWeb tasks were not significantly different ($U=49986$, $p=0.80$). The UnknownRetailer1 task was considered significantly less safe than both other tasks ($p<0.001$). Personal Banking data showed the same pattern: BankingApp and BankingWeb scenarios were not significantly different ($U=47718$, $p=0.04$), while UnknownRetailer2 was significantly less safe ($p<0.001$).

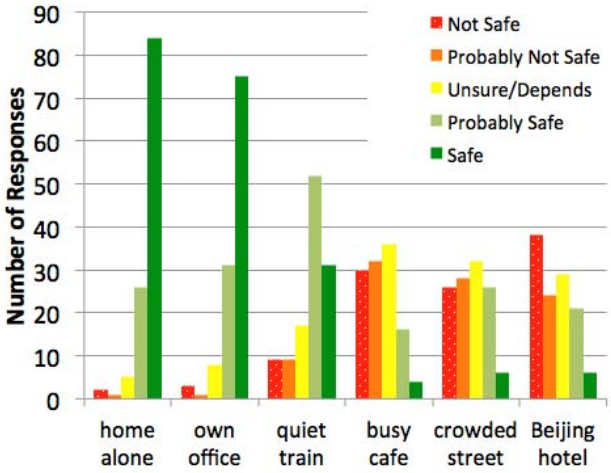

Figure 1. Perception of information safety in different environments when using a trusted app. For each environment, responses are ordered left to right from 'Not Safe' to 'Safe'.

3) Informed Risk Assessment

Participants were provided with little information about the scenarios, on which to base their decisions. They knew the type of environment, the task they would be performing, and in some cases whether other people were present. Table 1 details the items that were raised by more than one participant in response to the first open question: *"What else would you want to know about the situations described in this study to decide whether it is safe to access or enter sensitive information on your smartphone there?"* Response groups are derived from the coding process described above.

In all three groups, 36-55% of participants wanted to know more about the security of the network: who owned the network, what type of connection was being used (3G or Wifi), who else has access, and the likelihood of someone intercepting data transmitted over the network.

Doctors wanted to know that the network connection was secure (55%) but did not mention specific technologies or network features for achieving this. For IT Workers especially, use of VPN or encryption of data going over the network was an important factor (40%), with comments like *"I need to know if the information is encrypted"*. In contrast, Security Experts simply wanted to know who owned the network, and whether VPN was being used.

30% of IT Workers wanted more information about the remote service they would be accessing. This fell into two main categories: whether the service itself was honest, and whether it had adequate security. For instance: *"I would need some indication that the unfamiliar retailer/website used secure handling of the account information", "Is this a legitimate business?"* and *"if the website has any security certificates"*. Since the scenario given to Doctors was of doctors accessing medical records, none expressed a need to know more about the trustworthiness of the remote service.

Shoulder surfing was the primary threat identified by the Security Experts, but was mentioned by only 17% of IT Workers and 18% of Doctors. Given the low reported incidence of shoulder surfing risk in the field [17], the users' perception may be closer to the truth in this case.

No Personal Banking Consumer explicitly mentioned the risk of being observed. Instead they wanted information about the situation, for example "*how many people are around", "the demographic of the environments I am in",* and *"how close people are to me"*.

TABLE 1. PERCENTAGE OF IT WORKERS (IT), PERSONAL BANKING CONSUMERS (PB), AND DOCTORS (D) WHO WANTED TO KNOW EACH ITEM TO ASSESS WHETHER THEIR INFORMATION WOULD BE SAFE.

Information Wanted	IT	PB	D
Trust in the network connection	36	39	55
Trust in the remote service	30	37	0
Encryption of data over the network	40	19	9
Possibility of being observed	17	0	18
General information about the situation	0	13	0
Security of the device	8	4	18
Legal recourse or protection	0	4	0
Value/sensitivity of the information	6	0	0
Other people's experiences	0	4	0
Time and attention the task will take	0	4	0
Security of the application being used	4	0	9

Security of the device itself was another concern for some, with 8% of IT Workers, 4% of Personal Banking Consumers and 18% of doctors wanting more information about the device, such as whether it is caching data locally, whether other people have access to it, whether it may be infected with malware, and whether the screen lock is enabled.

There were two items requested by Security Experts that participants did not explicitly mention: whether they could delete data from the device, and the urgency of their need for the data.

4) Risks Perceived

According to the Security Experts, the scenarios presented in the questionnaire present the following possible risks (in the order they were given):

- Shoulder surfing, both direct and with cameras
- Man-in-the-middle attack, where communications are routed through an attacker
- Network snooping, where information is leaked from Bluetooth, WiFi or NFC networks
- Automatic backup of sensitive data to a cloud
- Data left on the device
- Loss or theft of the device

The broad categories of risk cited by the three participant groups are, in order of frequency: network risks, being observed, device risks, remote service risks, information loss risks, and risks associated with the situation (including environment). Table 2 illustrates for each of these categories the percentage of each group who mentioned at least one risk in that category. Each category is described in more detail below.

Network-related security risks, encompassing ways that information could be captured en route to a destination, were the most frequently mentioned for all three groups. 62% of IT Workers, 51% of Personal Banking Consumers and 20% of Doctors mentioned risks in this category, with the most frequently cited factors being:

- **Network snooping** (data intercepted as it travels over the network), e.g. *"Interception of wireless communication"* (29%/25%/20% in IT Worker/Personal Banking/Doctor groups respectively)
- **Insecure data transmission** (sensitive data sent without encryption) e.g. *"https or tunneling technology would make me feel more secure."* (21%/11%/0%)
- **Man-in-the-middle** (communications routed through an attacker) e.g. *"Even with https I suspect it is possible to interpose a proxy to terminate the https"* (12%/8%/0%)
- **Trust** (not knowing whether to trust the network) e.g. *"Confidential info traveling over the network"* (10%/4%0%)
- **Unsafe WiFi** (a WiFi network open to anyone) e.g. *"Public WiFi is usually unsecured"* (7%/8%/0%)

Observation risks involve information or passwords being observed while a device is being used. This was the second most common form of risk cited by IT Workers (60%) and Personal banking consumers (28%), and one of

TABLE 2: CATEGORIES OF SECURITY RISK PERCEIVED IN THE SCENARIOS BY IT WORKERS (IT), PERSONAL BANKING CONSUMERS (PB), AND DOCTORS (D), AND PERCENTAGE OF EACH GROUP IDENTIFYING AT LEAST ONE RISK IN THAT CATEGORY.

Type of Risk	Description	IT	PB	D
Network Risks	Risks encompassing ways that information could be captured en route.	62	51	20
Observation Risks	Information or passwords being observed while a device is being used.	60	28	30
Device Risks	Loss, theft, or obtaining data or login credentials directly from the device itself	52	13	30
Remote Service Risks	Risks related to the service being accessed (specifically the unknown retailer)	26	23	0
Loss of Information	Risk of information being lost or account access credentials being stolen	19	21	50
Situational Risks	Risks associated with the personal safety of the situation	10	6	0

the top three for Doctors (30%). Two forms of observation risk were mentioned.

- **Direct observation** (an observer near the user) e.g. *"people potentially looking at your screen"* (50%/26%/30%)
- **Indirect observation** (an observer at a distance using a camera, binoculars or other recording device) e.g. *"unobtrusive video surveillance watching my fingers on the phone"* (17%/26%/10%)

Device risks. The risk of a person obtaining data or login credentials directly from the device itself was the third most frequently cited form of risk in all groups (52%/13%/30%). These risks included:

- Theft (the user's device may be stolen) (26%/2%/10%)
- Loss (the user may lose their device, with the risk of someone else trying to access it) (12%/0%/30%)
- Malware (there may be software on the phone capturing user interactions and/or data transmissions) (14%/6%/0%)
- Hacking (someone may hack into the device) (7%/8%/0%)
- Storage of sensitive data (data may be stored on the device in unencrypted form) (7%/0%/0%)
- Physical access (an unauthorized person may access the phone) (7%/0%/0%)

Remote service risks. The IT Workers and Personal banking consumers identified risks related to the service being accessed (specifically referencing the unknown retailer), while the Doctors did not (26%/23%/0%). These risks were:

- **Untrusted service** (the service itself, and its trustworthiness, may be unknown) e.g. *"Entering credit cards on unknown websites is always a bad idea"*
- **Insecure service** (the service may not securely store data given to it) *"web site security"*
- **Dishonest service** (the service may misuse data given to it) e.g. *"the unfamiliar retailer is an obvious problem - who knows what they'll do with the CC info"*

Loss of information. Some participants (19%/21%/ 50%), including 50% of Doctors, described risks in terms of information being lost (10%/9%/20%) or account access credentials being obtained by a third party (12%/15%30%). For example, *"People are always looking for bank account information, credit card information, log in details."* or *"breach of privacy, access to personal information like SSN of pt or family information"*

Situational Risks. 10% of IT Workers and 6% of Personal Banking consumers mentioned risks associated with the personal safety of the situation, or safety in taking out a credit card. For example: *"I'm also worried about my own safety"*

5) Factors Influencing Decisions

The final open question was *"What factors affect your decision whether to access sensitive information in a given situation?"*

Network risks were the most frequently mentioned factors for both IT Workers (36%) and Personal Banking Consumers (39%). IT Worker participants (17% vs 6% for PB group) also commented specifically on measures to protect against network risk: *"can I enable VPN?"* or *"approved company security protections in place"*.

Observation risk was also an important factor in these groups (IT: 34%, PB: 28%). 26% of Personal Banking Consumers and 13% of IT Workers also considered the specific environment they were in, for example *"country I'm in"*.

Doctors' concerns when looking up medical data were quite different. The most cited factor, mentioned by 45% of the doctors, was time constraints, for example *"need access to critical test results anytime"*. Doctors also considered how important it was to access the data (27%), the time the transaction would take (27%), and the probability of data loss (18%).

No other factors were mentioned by more than 20% of the participants in any group.

6) Other Places of Concern

Personal Banking Consumers were asked whether there are other places they go where they would worry about accessing sensitive data on their smartphone. Their replies focused on public WiFi hotspots and the presence of other people, both as potential network snoopers and shoulder surfers. For instance:

> *"extremely crowded areas, but only if there was very little space between people."*
>
> *"Any public place with free wi-fi. those are the most dangerous places because your information can be hacked pretty easily by someone else that is using the wi-fi... and you wouldn't even know it!"*

V. DISCUSSION

A. Perceived Risks

Our data suggests that for many people, the possible risks of mobile transactions do not easily come to mind, or are not considered serious. This is consistent with prior work on ATM and Internet banking [8]. For some application areas, even when users are aware of risks, their need to perform the transaction can override security concerns. Where this is the case, the best security design is not likely to be achieved by

bringing users' understanding of risks to the level of security experts, but by accommodating the reality of users' situations.

In other situations, providing users with the information they need to make informed choices can enhance security. Participants wanted to know about network and observation/situational threats when deciding about information safety. These were the two sources of risk that were most salient. Participant comments about other places of concern (Section 3.5.8) also focused on the presence of others and untrusted WiFi access.

Perceived information safety largely aligns with physical safety, being strongly influenced by the presence of other people. We did not find evidence that familiarity confers an impression of safety – the crowded local street was not safer than a café in an unfamiliar neighborhood.

Consistent with Chin et al. [5], trust in the network was a key factor in assessing risk for all three groups, and one third of IT Workers and Personal Banking Consumers would consider the network risk before deciding to perform a transaction. In contrast, decision making for doctors was strongly driven by the urgency and importance of their need for the information. In all three groups, home and office environments (and networks) were considered relatively safe. Trust in home networks may not always be justified when administered by non-experts [37].

The IT Workers were familiar with using laptops to access company information remotely, and VPN connections to make this access secure. They had company training in keeping sensitive information secure. IT Workers were much more likely to use a lock on their smartphone (63%, excluding respondents who had a company-required lock in place), compared to 41% of Personal Banking consumers, which is consistent with the findings of other studies (e.g. 47% in [6]).

Two thirds of IT Workers and one third of Personal Banking Consumers and Doctors listed shoulder surfing as a risk, and one third of IT Workers and Personal Banking Consumers said they would take this into account when deciding whether to perform a transaction. The difference between the awareness of observation risk, and the stated influence of this risk on decision-making could be explained by the controllability, or voluntariness of the risk (as defined by Lowrance [28]). Participants commented that they could take steps to reduce this risk by choosing their position in the space (e.g. *"Usually I try to keep my back to a wall"*), or shielding their screen, and some noted that this was easier to do with a mobile device than a laptop.

Most participants did not mention the digital security of their mobile device – fewer than 15% listed concerns about the device being infected or hacked into, both of which were possible risks. The possible risk of cloud storage of data was not a concern, consistent with previous findings that smartphone users were not concerned about their data being stored on servers [13].

Given peoples' natural tendency to associate risk with physical threats [14], and press coverage of smartphone-related crime, the low concern about device theft is perhaps surprising. Contrast this with Chin et al's finding that physical phone loss was a primary concern in relation to smartphone use in general [7]. It is possible that because of the security measures they had in place (phone lock, remote wipe capability, company-approved app), they did not consider their information to be at great risk if they lost their phone, or it was snatched.

B. Design Implications

If organizations wish to promote secure behavior in their employees or customers (users) when using mobile devices, it is important to identify the security risks and adjust the app design to identify, mitigate and/or communicate the risk. If users are already aware of the risks, but choosing not to act, then a different approach is needed. For example, corporations can opt for a fail-safe security option where users are denied access in case of non-compliance.

More specifically, there needs to be a balance between security and usability based on the value of the resources at risk and the cost of preventing access. For high value resources, fail safe (e.g., no access, require management consent) may be most appropriate. Low value resource access may be approved but audited for compliance and post incident risk assessment. If the organization doesn't have the ability to discriminate between high and low value resources and risk (or gradations in between), the default may be to assume the value at risk is high.

The primary risks identified by the study are around network security, shoulder surfing, device / data loss, and "hacking". We now discuss mobile app design options to address these risk factors.

Effectively communicating network security risk is in general very challenging. Our data also suggest that other concerns may override security concerns, in which case risk communication will provide little benefit. An alternative design choice is to eliminate as much user interaction as possible. Instead, rely on system level enforcements. For example, apps should embed logic to verify network security, either by ensuring that the VPN network connection has been properly established, or by using SSL certificate pinning. If the network connection is not as expected (e.g., possible man-in-the middle), attempt alternative network options, such as establishing a VPN connection. Otherwise, report the security problem and deny access.

Since users may not consider shoulder surfing threats, it may be possible to provide some automated threat detection through the device camera or microphone. This could be translated into protective actions on the device, such as switching to a non-observable authentication method.

Given the low use of device locking mechanisms, protecting data loss on mobile devices may call for additional security mechanisms to address device loss, theft or insider attack. The first is to recognize when the user is not present with the device. This can be as simple as a device or app lock-out when the device is inactive for a period of time. Passive authentication techniques, including how the device is being held and interaction (swipes) on the screen are continuous authentication techniques that might be employed. Also, rather than relying on on-device authentication methods, network-centric authentication will

make it more difficult for the attacker to simply manipulate the device to gain access to network-based resources. A combination of local on-device and network-centric authentication techniques may make the applications and data more secure. Finally, Mobile Device Management (MDM) solutions typically allow for remote wipe of the device or application content if the device is lost.

Hacking covers multiple security risks, including some of the issues discussed above. Several technologies are typically needed to provide device protection. This includes firewalls, anti-virus and intrusion detection/prevention. This is typically integrated with the platform rather than on a per-app basis. Those aspects of "hacking", which include network compromise and device compromise due to theft, are discussed above.

C. Limitations and Further Work

These results are based on questionnaires, in which participants were given partial information about a situation and asked to consider the risks. Although risk perception reports can be more reliable predictors of actual behavior than what people say they will do [20], responses may still differ from the risks perceived and factors considered by users in a transaction performed in a real mobile environment. Furthermore, since the incentive for the Personal Banking group encouraged them to report more risks, their actual level of concern may be overestimated here. This study does not demonstrate whether these factors would be predictive of actual decisions people make. For example, our emphasis on information safety ignores other factors that are important in mobile risk perception and decision-making, such as personal safety. A complementary study could query participants about perceived risks when they are in environments they normally visit. This would provide data from real environments, without the potential bias introduced by describing the presence or absence of others in an imagined scenario, but it would not be easy to systematically explore factors like the presence of other people, or the familiarity of the environment, as we have begun to do here.

Other environments such as malls, restaurants and airports may bring new risks to mind that were not captured in these studies. It would also be valuable to tease apart the impacts of the factors that participants identified as important, especially network security and the presence of other people.

To increase the generalizability of our results, we explored seven different usage scenarios within three different user groups. This revealed many similarities but also some differences in thinking between the groups. Other groups and scenarios may reveal new concerns not described here. The group of Doctors was small, and those findings require further validation.

Many of the same risks are valid for other devices, but the capabilities, vulnerabilities and usage environments of mobile devices are different than for laptop/desktop systems, and people perceive risks differently for laptop/desktop devices than mobile devices [13]. In our results, the perceived most risky environments were those where a desktop system would never be used.

We did not ask participants about their exposure to the various risks, through personal experience, anecdote or media reports. Thus, we cannot assess the extent to which these risk assessments may have been influenced by, or generalized from prior positive or negative experiences.

VI. Conclusions

Achieving both usability and security in mobile contexts requires a balance of contribution between system and user. However, users are unlikely to guard against risks that do not come to mind in typical mobile device usage. To inform the design of mobile applications, we have presented a user study of perceived risk in mobile transactions incorporating three user groups: information technology workers accessing company data; consumers using mobile personal banking; and doctors accessing medical records. Our study found overall low levels of reporting of possible information security threats, including device theft and loss. Furthermore, participants' understanding of network threats is very different to that of experts. In our study, we found that assessment of risk was influenced by the origin of the content being accessed and the presence of other people nearby, but not by whether the access was through a trusted app or a mobile browser. This exposes users to danger from phishing attacks and other network threats.

Risks that are important to organizations but do not come readily to the minds of users include device theft and loss, malware, device hacking and cloud/device storage of data. Given this context, organizations would be wise to design for built-in, non-intrusive security mechanisms such as passive authentication techniques and automated malware scanning. These findings also suggest ways that organizations could tailor communication with employees and customers to address common concerns.

Finally, these findings suggest a strong need for organizations to understand the broader context of user decisions about security when using their mobile device for sensitive transactions, and design for usable security. By understanding perceived risks, we can identify opportunities to bridge the gap between the severity of a security threat and users' understanding of the risk associated with that threat, and thereby improve the overall usability and security of mobile services.

ACKNOWLEDGMENT

This work was partially supported by a grant from the United States Department of Homeland Security under contract FA8750-12-C-0265.

References

[1] C. Amrutkar, P. Traynor, and P. van Oorschot. "An empirical evaluation of security indicators in mobile web browsers", IEEE Transactions on Mobile Computing, vol. 99, no. PrePrints, p. 1, 2013.

[2] C. Bravo-Lillo, S. Komanduri, L.F. Cranor, R.W. Reeder, M. Sleeper, J. Downs, and S. Schechter. "Your attention please: designing security-decision UIs to make genuine risks harder to ignore". Symposium on Usable Privacy and Security 2013.

[3] P. Blythe, J. Camp, and, V. Garg. "Targeted risk communication for computer security". Proceedings of the 16th international conference on Intelligent user interfaces, 2011, pp. 295-298.

[4] Camp, L. J., "Mental models of privacy and security". SSRN: http://ssrn.com/abstract=922735, 2006.

[5] E. Chin, A. Felt, V. Sekar, and D. Wagner, D. "Measuring user confidence in smartphone privacy and security". Symposium on Usable Privacy and Security 2012.

[6] Confident Technologies. Mobile (In)Security: A Survey of Security Habits on Smartphones and Tablets. September 2011. Downloaded April 2013 from: http://confidenttechnologies.com/content/mobile-security-survey-results-0

[7] Consumer Reports. Smart phone thefts rose to 3.1 million last year. ConsumerReports.org. Accessed March 2016 at: http://www.consumerreports.org/cro/news/2014/04/smart-phone-thefts-rose-to-3-1-million-last-year/index.htm

[8] Davinson, N. and Sillence, E. "Using the health belief model to explore users' perceptions of 'being safe and secure' in the world of technology mediated financial transactions", International Journal of Human-Computer Studies, Available online March 2016, ISSN 1071-5819, http://dx.doi.org/10.1016/j.ijhcs.2013.10.003

[9] J. Downs, M. Holbrook, S. Sheng, and L. Cranor. "Are your participants gaming the system? Screening Mechanical Turk workers". Proc. CHI 2010. ACM Press, New York, pp. 2399-2402.

[10] S. Egelman, L. F. Cranor, and J. Hong. "You've been warned: an empirical study of the effectiveness of web browser phishing warnings". CHI 2008, pp. 1065-1074. ACM

[11] European Association for Visual Data Security, 2013. New survey highlights risks from 'commuter snoopers'. Secure. Accessed March 2016 at: http://www.visualdatasecurity.eu/2013/10/new-survey-highlights-risk-commuter-snoopers/

[12] Federal Communications Commission. 2012. Announcement of new initiatives to combat smartphone and data theft. Accessed March 2016 at: http://www.fcc.gov/document/announcement-new-initiatives-combat-smartphone-and-data-theft

[13] A. Felt, S. Egelman, and D. Wagner. "I've got 99 problems, but vibration ain't one: A survey of smartphone users' concerns". SPSM 2012, ACM Press.

[14] V. Garg and J Camp. "End user perception of online risk under uncertainty". HICCS 2012. IEEE. pp. 3278-3287.

[15] C. Herley. "So long, and no thanks for the externalities: the rational rejection of security advice by users". NSPW '09, pp. 133-144, ACM. http://dl.acm.org/citation.cfm?id=1719050

[16] A. Herzberg and A. Jbara. "Security and identification indicators for browsers against spoofing and phishing attacks", ACM Transactions on Internet Technology (TOIT), Volume 8 Issue 4, September 2008

[17] M. Harback, E. Zezschwitz, A. Fichter, A. De Luca, and M. Smith. "It's a hard lock life: A field study of smartphone (un)locking behavior and risk perception". Symposium on Usable Privacy and Security 2014, USENIX. pp 213-230.

[18] D. Huang, P. Rau, G. Salvendy, X. Shang, Y. Liu, and X. Wang. 2008. "Perception of information security and its implications for mobile phone". HFES '08. pp. 1650-1655.

[19] D. Kahneman, P. Slovic, and A. Tversky. Judgment under uncertainty: Heuristics and biases. Cambridge University Press, 1982.

[20] M. Keith, S. Thompson, J. Hale, P. Lowry, and C. Greer. 2013. "Information disclosure on mobile devices: Re-examining privacy calculus with actual user behavior". Int. Journal of Human-Computer Studies 71 pp. 1163-1173, 2013.

[21] I. Kirlappos, and M.A. Sasse. "Security education against Phishing: A modest proposal for a major rethink". IEEE Security and Privacy Magazine 10(2), pp. 24-32, 2012.

[22] I. Kirlappos, M.A. Sasse and N. Harvey. "Why trust seals don't work: A study of user perceptions and behavior". In S. Katzenbeisser, E. Weippl, L. Camp, M. Volkamer., M. Reiter, X. Zhang. (Eds.). Trust and Trustworthy Computing 7344, 308-324. Berlin/Heidelberg: Springer. 2012.

[23] P. Klasnja, S. Consolvo, J. Jung, B. Greenstein, L. LeGrand, P. Powledge and D. Wetherall. "When I am on Wi-Fi, I am fearless: privacy concerns & practices in everyday Wi-Fi use". In CHI 2009. ACM, New York, NY, USA, 1993-2002.

[24] K. Krol, M. Moroz, and M.A. Sasse. "Don't work. Can't work? Why it's time to rethink security warnings". CRiSIS 2012, pp. 1 – 8.

[25] J.R. Landis and G.G. Koch. The measurement of observer agreement for categorical data. Biometrics 33:159-174. 1977.

[26] D. LeBlanc R. and Biddle. "Risk perception of internet-related activities". Tenth Annual International Conference on Privacy, Security and Trust. 88-95, IEEE. 2012.

[27] Lookout. Lookout projects lost and stolen phones could cost U.S. consumers over $30 billion in 2012. 2012. Accessed March 2016 at: https://www.lookout.com/news-mobile-security/lookout-lost-phones-30-billion

[28] W. Lowrance. Of acceptable risk: Science and the determination of safety. William Kaufmann. 1976.

[29] I. Muslokhov, Y. Boshmaf, C. Kuo, J. Lester and K. Beznosov. "Know your enemy: The risk of unauthorized access in smartphones by insiders". Proc. MobileHCI '13. ACM Press, 271-280. 2013.

[30] J. Ross, L. Irani, M. Silberman, A. Zaldivar and B. Tomlinson. "Who are the crowdworkers? Shifting demographics in Mechanical Turk". Extended Abstracts of CHI 2010. ACM Press.

[31] S. Sheng, M. Holbrook, P. Kumaraguru, L.F. Cranor and J. Downs. "Who falls for phish?: A demographic analysis of phishing susceptibility and effectiveness of interventions". CHI 2010, 373-382, ACM New York, NY, USA.

[32] J. Sobey, R. Biddle, P.C. Van Oorschot, and A.S. Patrick. "Exploring user reactions to browser cues for extended validation certificates". Proc. ESORICS 2008, LNCS 5283, 411-427. NRC 50412.

[33] Symantec. The Symantec Smartphone Honey Stick Project. 2012. Accessed March 2016 at: http://www.symantec.com/content/en/us/about/presskits/b-symantec-smartphone-honey-stick-project.en-us.pdf

[34] A. Tversky and D. Kahneman. "Judgment under uncertainty: Heuristics and biases". Science, Vol. 185, 1124-1131. 1974.

[35] A. Tversky and D. Kahneman. "The framing of decisions and the psychology of choice", Science, No. 4481, Vol. 211, pp. 453-8. 1981.

[36] J. Uffen, N. Kaemmerer and M. Breitner. "Personality traits and cognitive determinants — An empirical investigation of the use of smartphone security measures". Journal of Information Security 2013 (4), pp 203-212.

[37] R. Wash. Folk models of home computer security. Proc. SOUPS '10. ACM, New York. 2010.