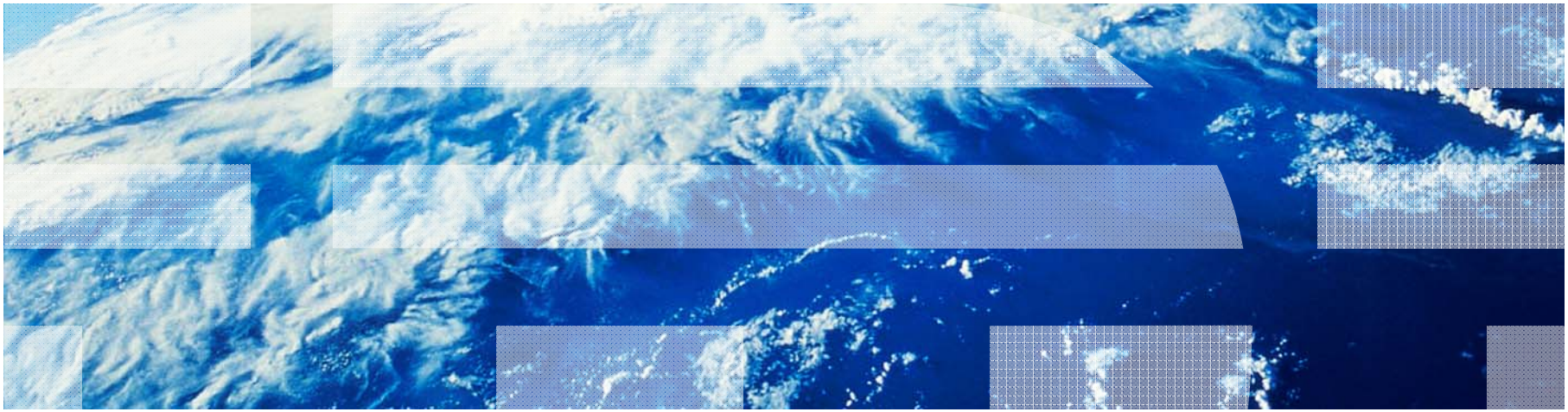
Perceptions of Risk in Mobile Transactions

Shari Trewin, Cal Swart, Larry Koved and Kapil Singh

IBM T.J. Watson Research Center

This work is supported in part by a grant from the Department of Homeland Security under contract FA8750-12-C-0265.



Mobile Security Technologies (MoST) 2016

More and More, We Use Mobile Devices for Sensitive Transactions What are the Risks?

- Theft
  - Smartphone theft accounted for 30-40% of all crime in major US Cities in 2012.
  - 3.1 million smartphones stolen in 2013 in the US
- Loss
  - Average American consumer loses their phone once every year
  - 90% of people picking up lost smartphones will try to access sensitive data
- Shoulder surfing
  - 2/3 (Europe) – 3/4 (UK) of commuters look at what others are doing on their devices
- Malware attacks – 10% of Android devices every 3 months in the US [SophosLabs 2013]
- Network snooping
- Insider attack
  - 12% of participants in one study

"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."

Tversky and Kahneman, Judgment Under Uncertainty, 1974

Research Questions

1. Does the location have an effect on perceived information safety?
2. What risks do come to people's minds, when performing sensitive transactions on a mobile device?
3. What information do people use to decide whether it is safe?
4. What factors influence the decision to perform a sensitive transaction on a mobile device?

Three User Groups

(IT) Information Technology workers

(PB) Personal banking consumers
(Amazon Mechanical Turk)

(D) Doctors

Reference group:

- IT Security Experts

Six locations

At home by yourself

In a crowded local street

On a quiet train at night with no-one nearby

In your office at your desk

In a very busy café in an unfamiliar neighborhood

In a Beijing hotel room

Three mobile tasks

For IT Workers & Security Experts

- Use company app to look up information about an unannounced acquisition
- Look up your personal retirement benefit information on a trusted 3rd party web site
- Make a $100 emergency purchase using the web site of an unfamiliar retailer entering your company's credit card information

For Personal Banking – using your mobile device:

- Look up your account balance using the bank's app
- Look up your account balance on the bank's web site
- Make a $100 emergency purchase using the web site of an unfamiliar retailer entering your credit card information

Doctors

- Use a standards compliant (HIPAA) medical app to access your patients' medical record

Would [your / the] information be safe if you did that in these places?

Method – Open Questions

"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, such as the type of network connection or presence of other people.

"What, if any, are the security risks you see in these situations?"

- Responses here indicate the specific threats that the individuals are aware of, such as device theft or network eavesdropping.

"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, such as the urgency of the need to access the information, and ability to go to a safer place.

Method – Open Questions Analysis

- An initial set of codes was derived for each question by starting from the responses given by the IT security experts, and adding or subdividing codes as necessary to cover themes emerging from the remainder of the data.

- The three open questions were analyzed by post-coding all responses from IT Workers and Individuals.
  - Two independent coders.

- After the independent coding, for each question, an inter-rater reliability analysis using the Kappa statistic was performed to determine consistency between the coders. After two iterations of coding, the Kappa values achieved were:
  - *'what else'* question, Kappa = 0.875 ($p < .0.001$);
  - *'security risks'* question, Kappa = 0.917 ($p < .0.001$);
  - *'what factors'* question, Kappa = 0.879 ($p < .0.001$).

- Items coded inconsistently were discarded from further analysis.
  - For the *'what else'* question we threw out 20% (51 out of 258 comments).
  - For the *'security risks'* question we threw out 8% (24 out of 297 separate comments) of the data.
  - For the *'what factors'* question we threw out 11% (30 of 261 separate comments).

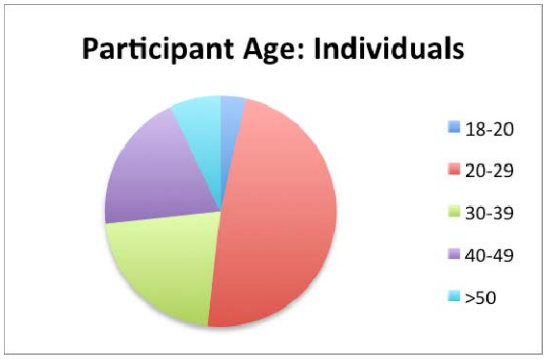
Method and Participants - IT Workers

- **Method**
  - Questionnaire distributed on paper and web form at a tech company
    - Distributed shortly after annual certification of business conduct guidelines
      - Protection of company data was fresh in their minds
  - Limited to participants who owned a smartphone > 6 months

- **Participants**
  - 46 male, 7 female. Mean age = 44.7, (Range 23-67, Std dev. = 12.4).
  - Self reported security expertise:
    1=minimal, 26=average, 24=knowledgeable, 2=expert

Method and Participants - Personal Banking

- Methods
  - Questionnaire on Amazon Mechanical
  - Limited to *Turkers* who had at least 1000 completed “tasks” with at least 95% tasks accepted as quality work
  - US-based workers (for legal reasons)
  - Three test questions to ensure Turkers had read and understood the scenario
  - Limited to participants who owned a smartphone > 6 months
- Participants
  - 54 of 76 respondents qualified (owned a smartphone > 6 months)
    - 38 male, 16 female
    - Device ownership: 34 Android, 20 iPhone, 2 Blackberry, 1 other
    - Device unlock: 12 4-digit PIN, 5 gesture, 22 swipe, 10 no lock, 5 PIN (unspecified length)



Method and Participants – Doctors*

- Method
  - Paper questionnaire
    - Included risk perception questions
- Participants
  - 11 hospital-affiliated doctors (10 male)
    - A range of different specializations
    - All were smartphone users
- Identified needs and current practices

**Not funded by the Department of Homeland Security*

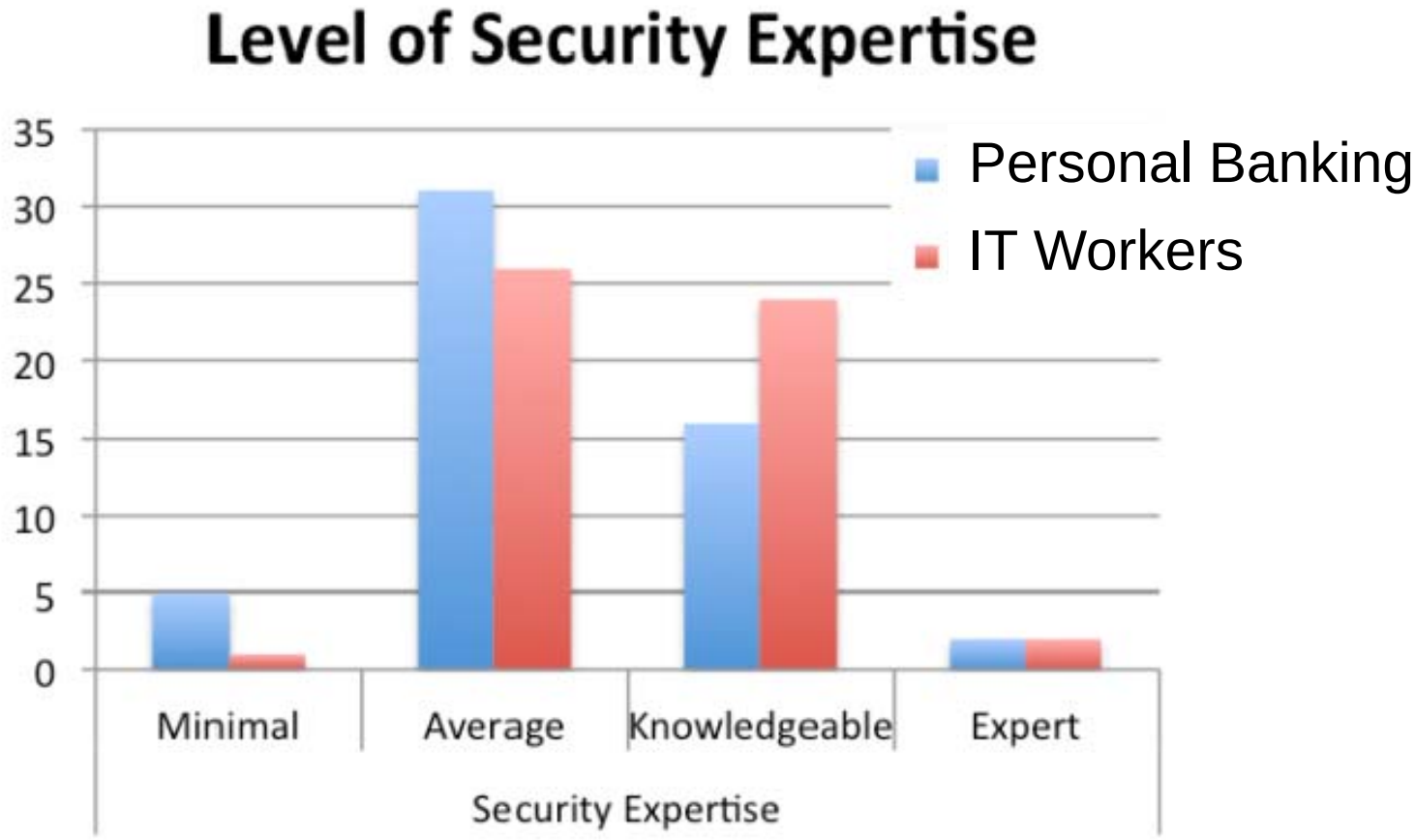
Method and Participants - Security Experts

- **Method**
  - Group discussion using the same materials as the IT workers

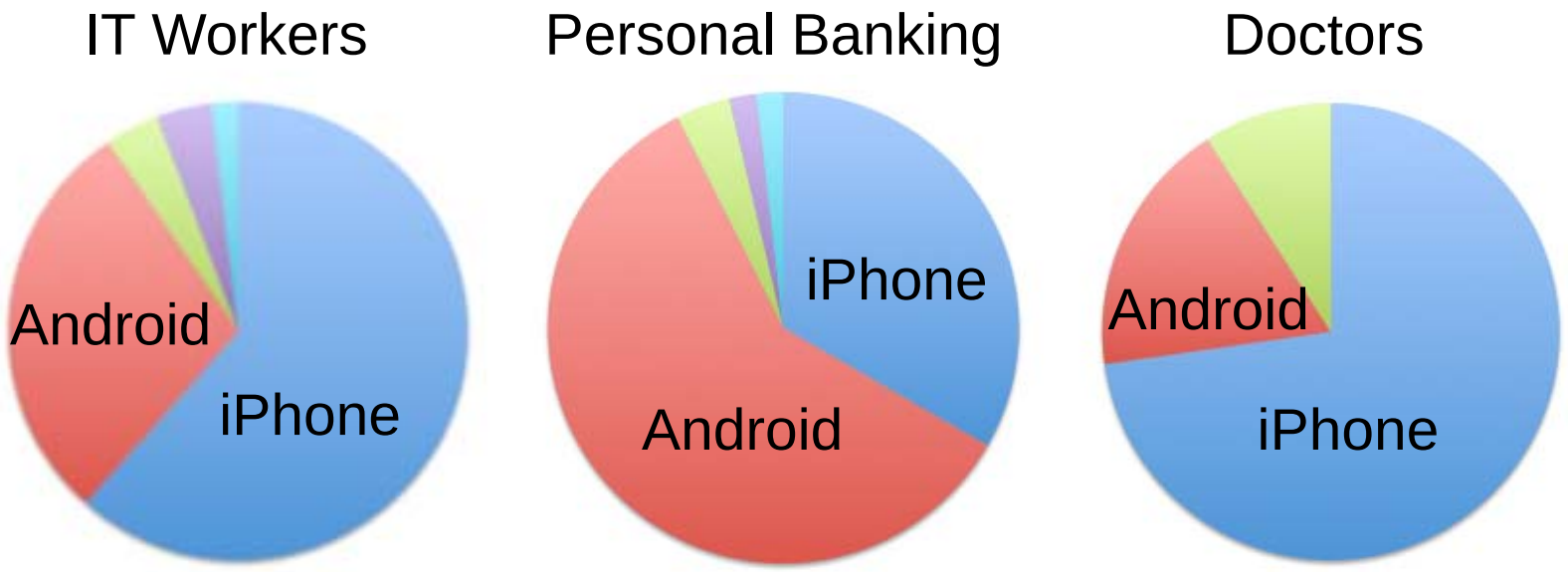
- **Participants – IT Security Experts**
  - 11 security researchers
  - all male
  - 10 with over 10 years of IT security research experience, one with 5 years of experience

Contrasting the user groups

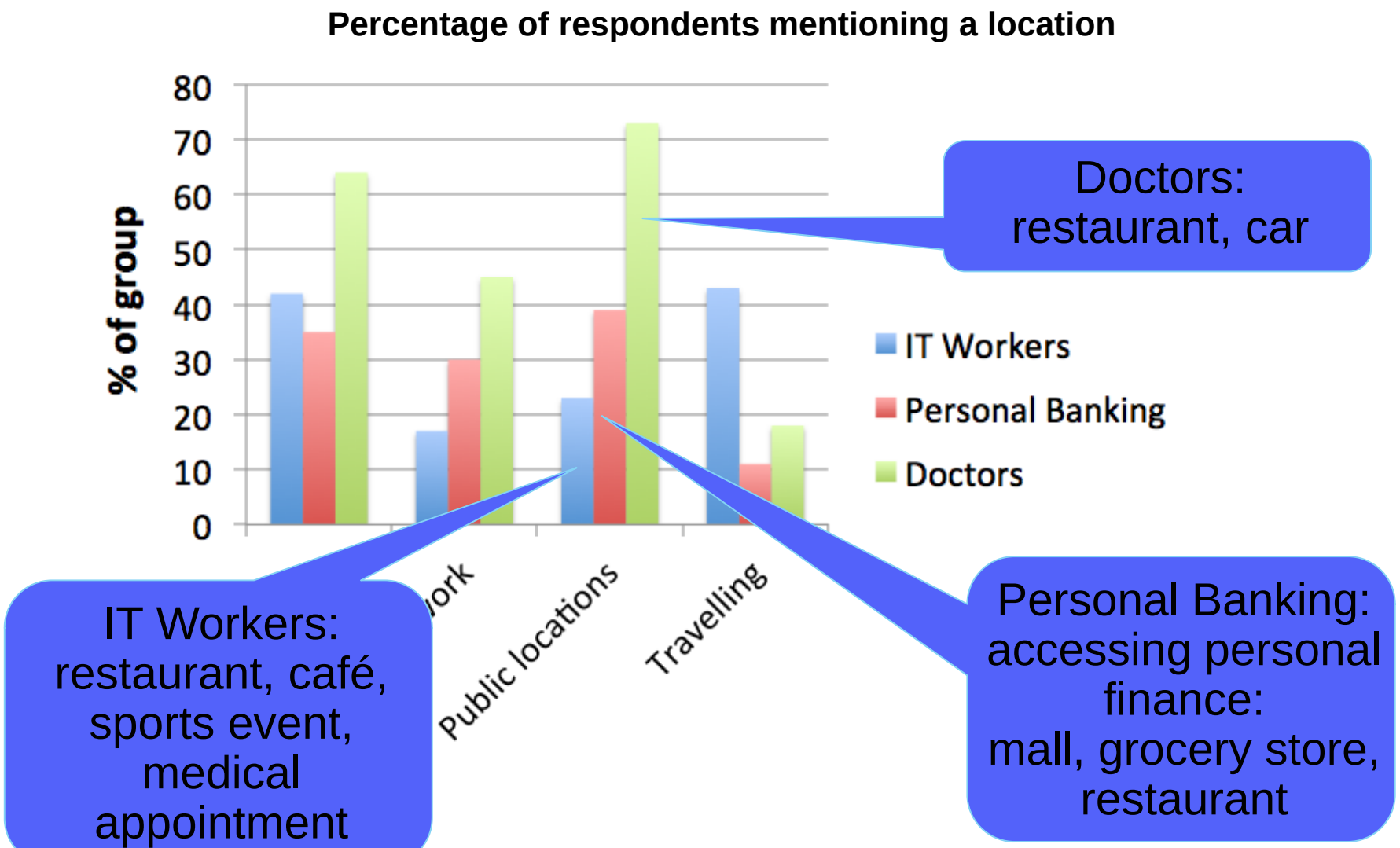
Self-reported security expertise for IT Workers and Personal Banking



Mobile Devices Owned



Locations for Mobile Access



Use of Phone Lock

Overall, 54% locked their phones

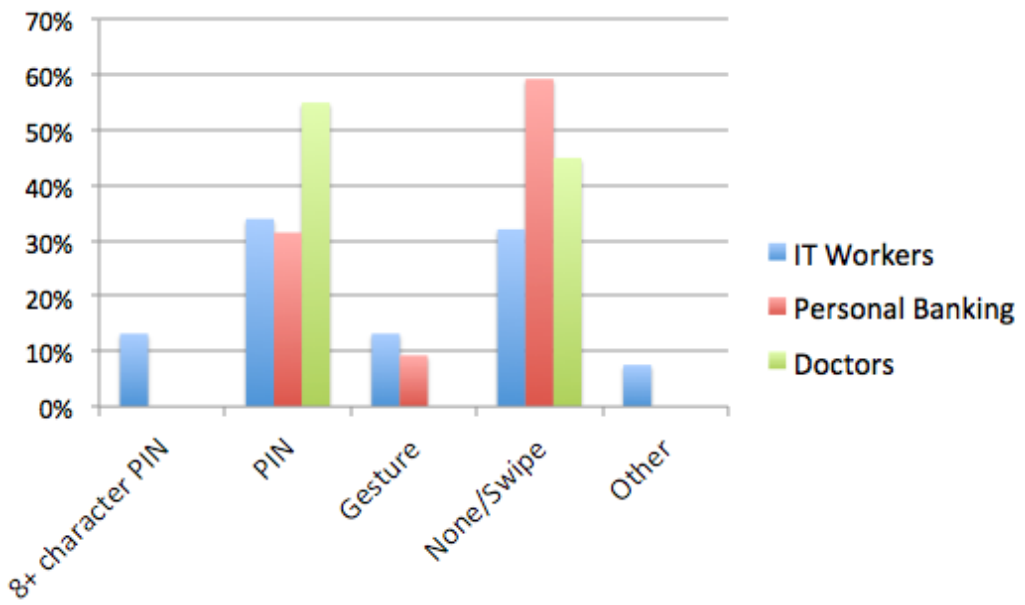
IT Workers: 68%

- 57% of women
- 70% of men
- 63% if corporate data users are excluded

Personal Banking: 41%

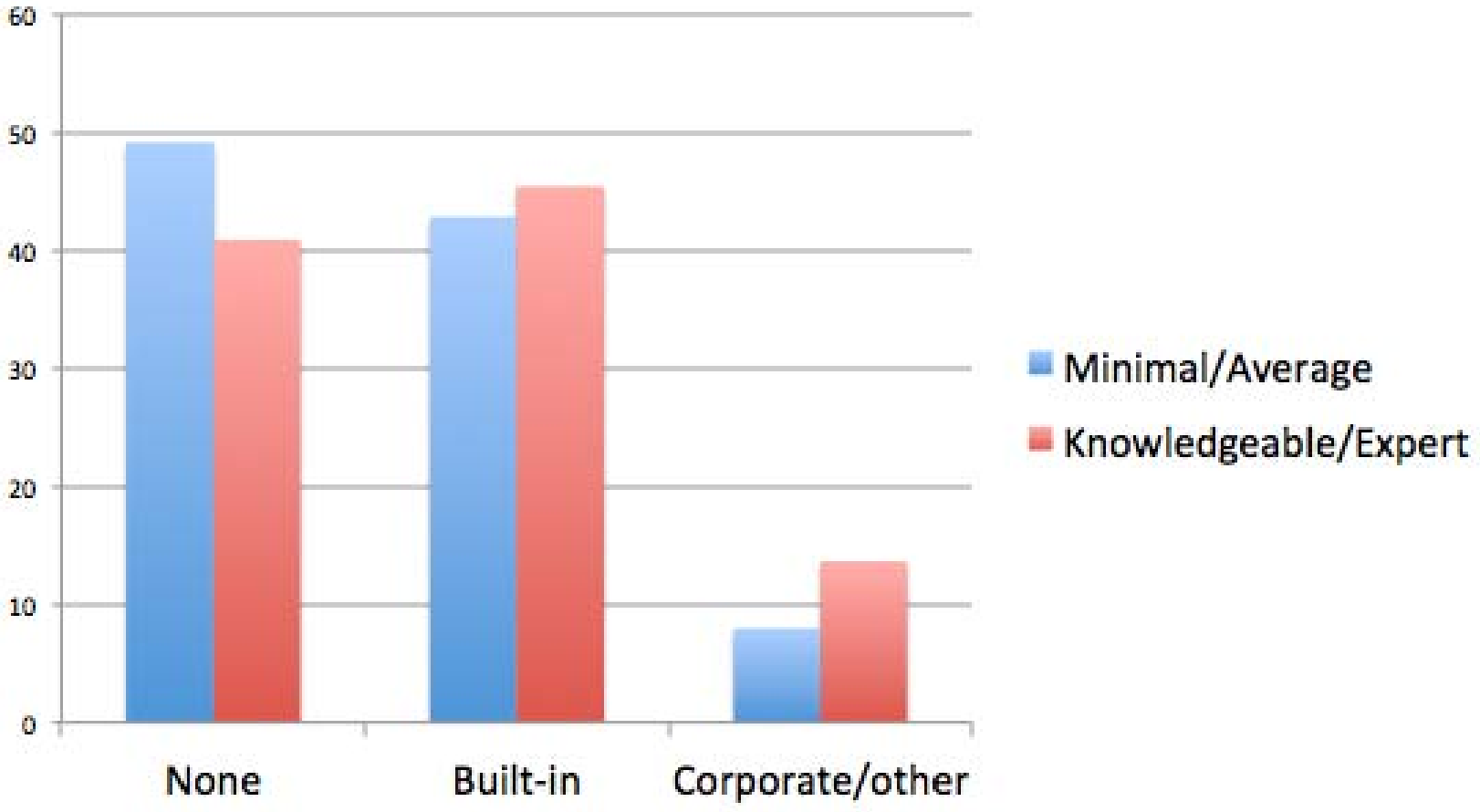
- 53% of women
- 37% of men

Doctors: 55%



Security Expertise and Phone Locking

No strong expertise effect

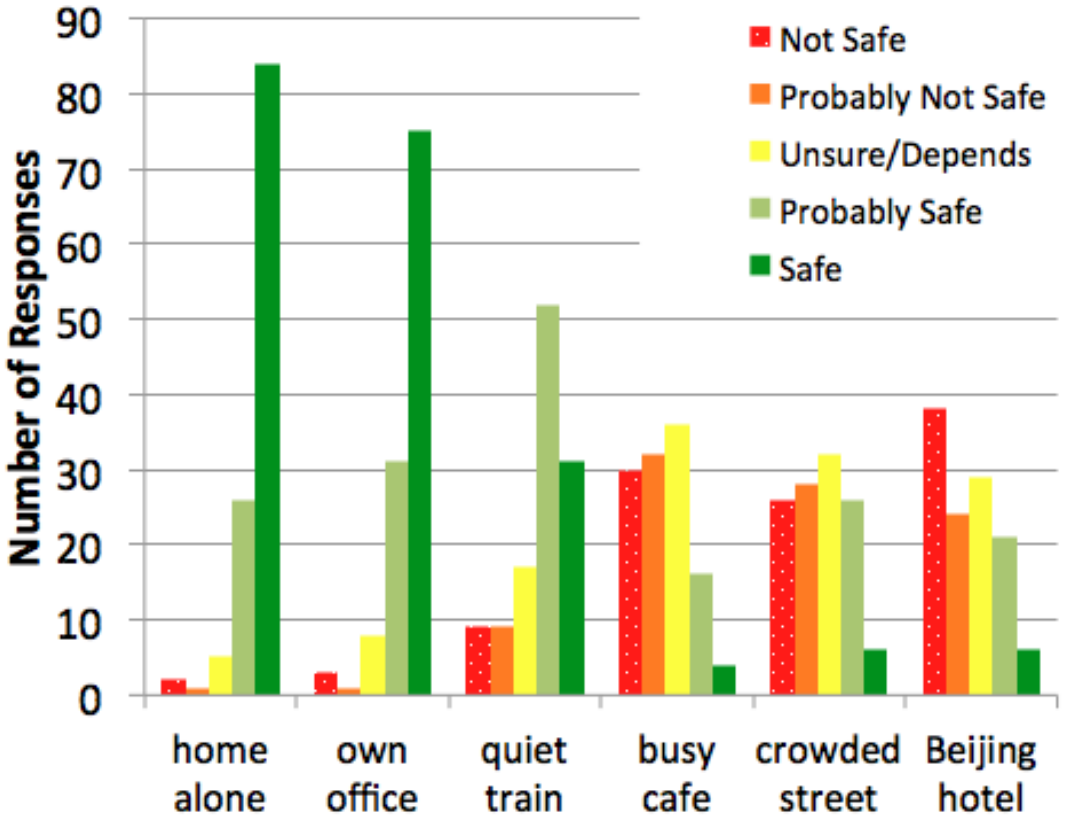


Research Questions

1. Does the location have an effect on perceived information safety?
2. What risks do come to people's minds, when performing sensitive transactions on a mobile device?
3. What information do people use to decide whether it is safe?
4. What factors influence the decision to perform a sensitive transaction on a mobile device?

Significant effect of location on perceived information safety

- Using a trusted app (company info, personal banking, medical records)
- Kruskal-Wallis Chi-Square=329, df=5, p<0.001

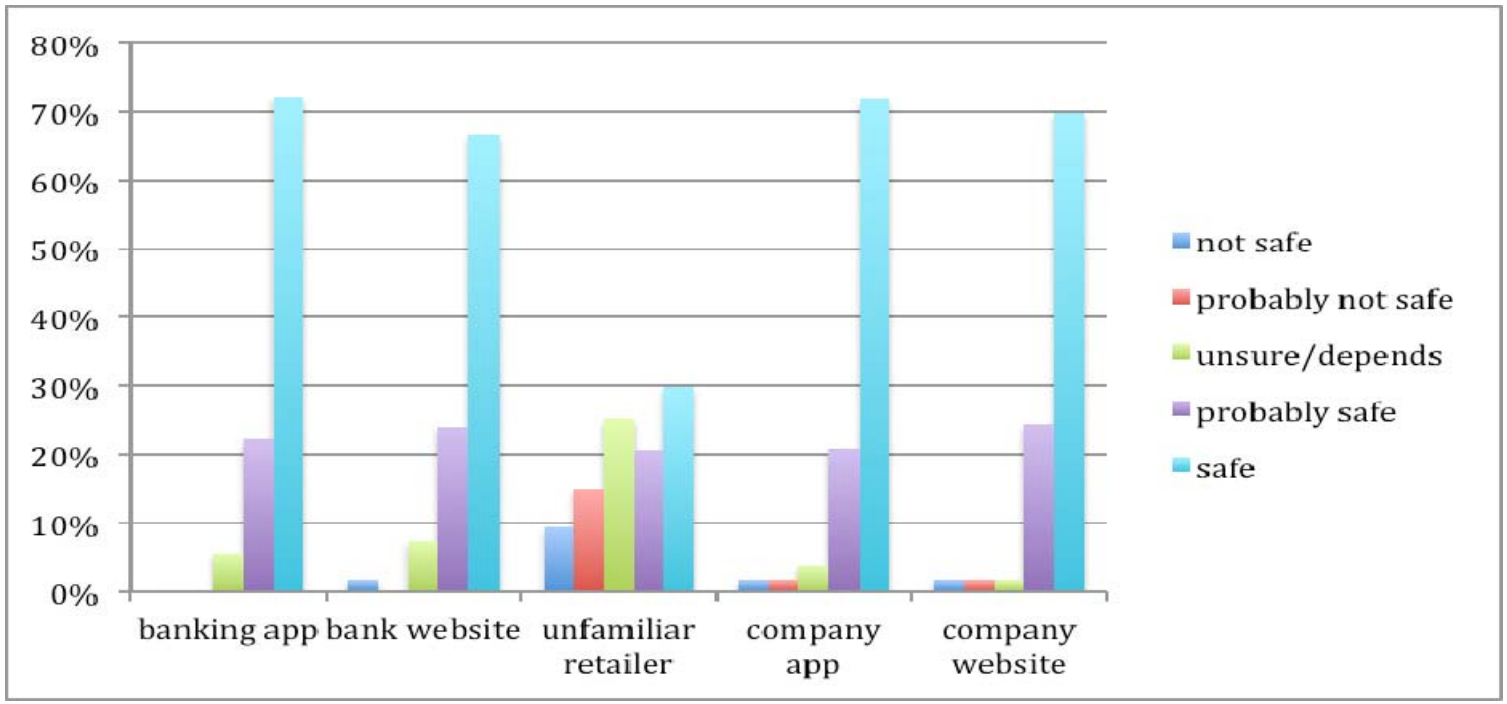


Perception of information safety in different locations when using a trusted app

Risk Assessments – Information Safety by Task when Home Alone

- Significant effect on assessments of safety
  - Kruskal-Wallis test, Chi-square = 67.995, $p<0.001$.

- Pairwise comparisons with Bonferroni correction to adjust for multiple tests indicate that the 'unfamiliar retailer' is significantly different from all other tasks
  - Mann-Whitney test, $p<0.001$
- No other differences are significant ($p>0.4$ in all cases)



Summary of responses indicating safety of different transaction types performed from home

Research Questions

1. Does the location have an effect on perceived information safety?
2. What risks do come to people's minds, when performing sensitive transactions on a mobile device?
3. What information do people use to decide whether it is safe?
4. What factors influence the decision to perform a sensitive transaction on a mobile device?

What risks come to mind?

"What, if any, are the security risks you see in these situations?"

- IT Security Experts identified the following security risks in the scenarios.
  Risks are presented in the order they were provided:
  - Shoulder surfing – direct observation of either sensitive information or passwords, potentially using a camera from a distance
  - Man in the middle attack – where communications are routed through an attacker
  - Network snooping – leaking information from Bluetooth, WiFi or NFC networks
  - Automatic backup of sensitive data to a cloud owned by an external organization
  - Data left on the device – vulnerable if the device is compromised, stolen, or used by another person.
  - Loss or theft of the device

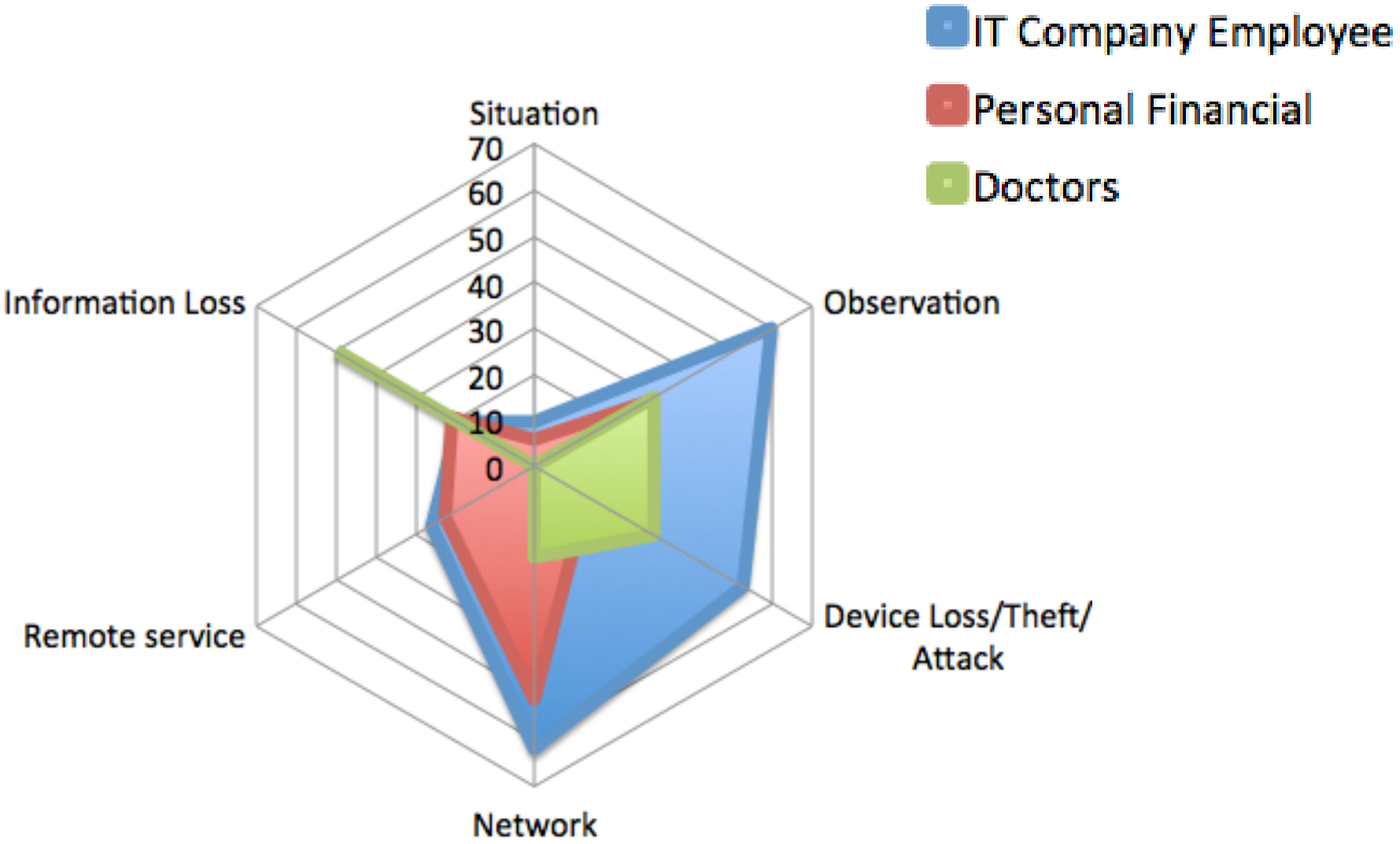
What risks come to mind?

"What, if any, are the security risks you see in these situations?"

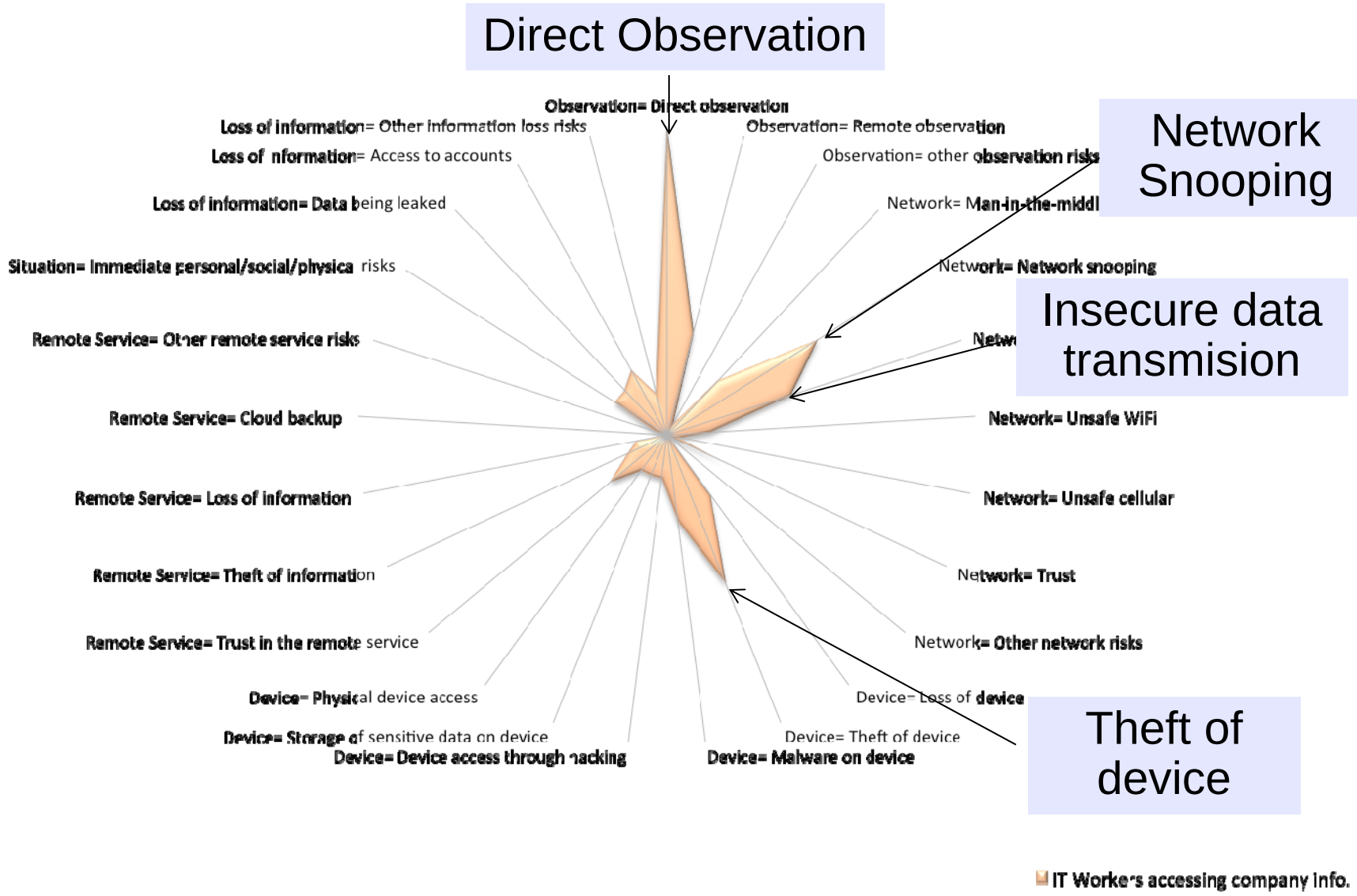
Type of Risk	Description	IT	PB	D
Network Risks	Risks encompassing ways that information could be captured en route to a destination.	62	51	20
Observation Risks	Information or passwords being observed while a device is being used.	60	28	30
Device Risks	Loss, theft, or otherwise obtaining data or login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

Percentage of each group mentioning a type of risk

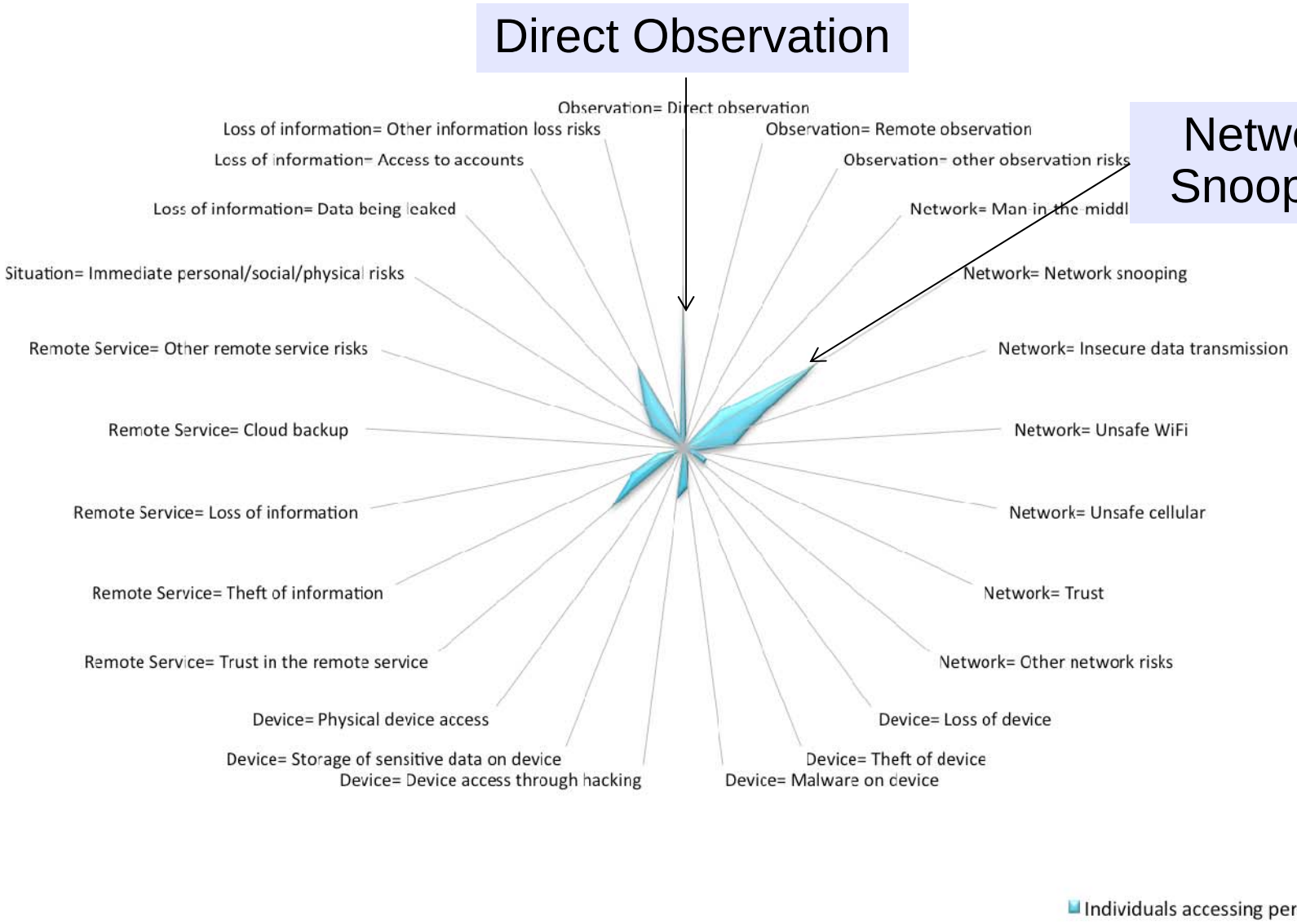
Perceived Risk



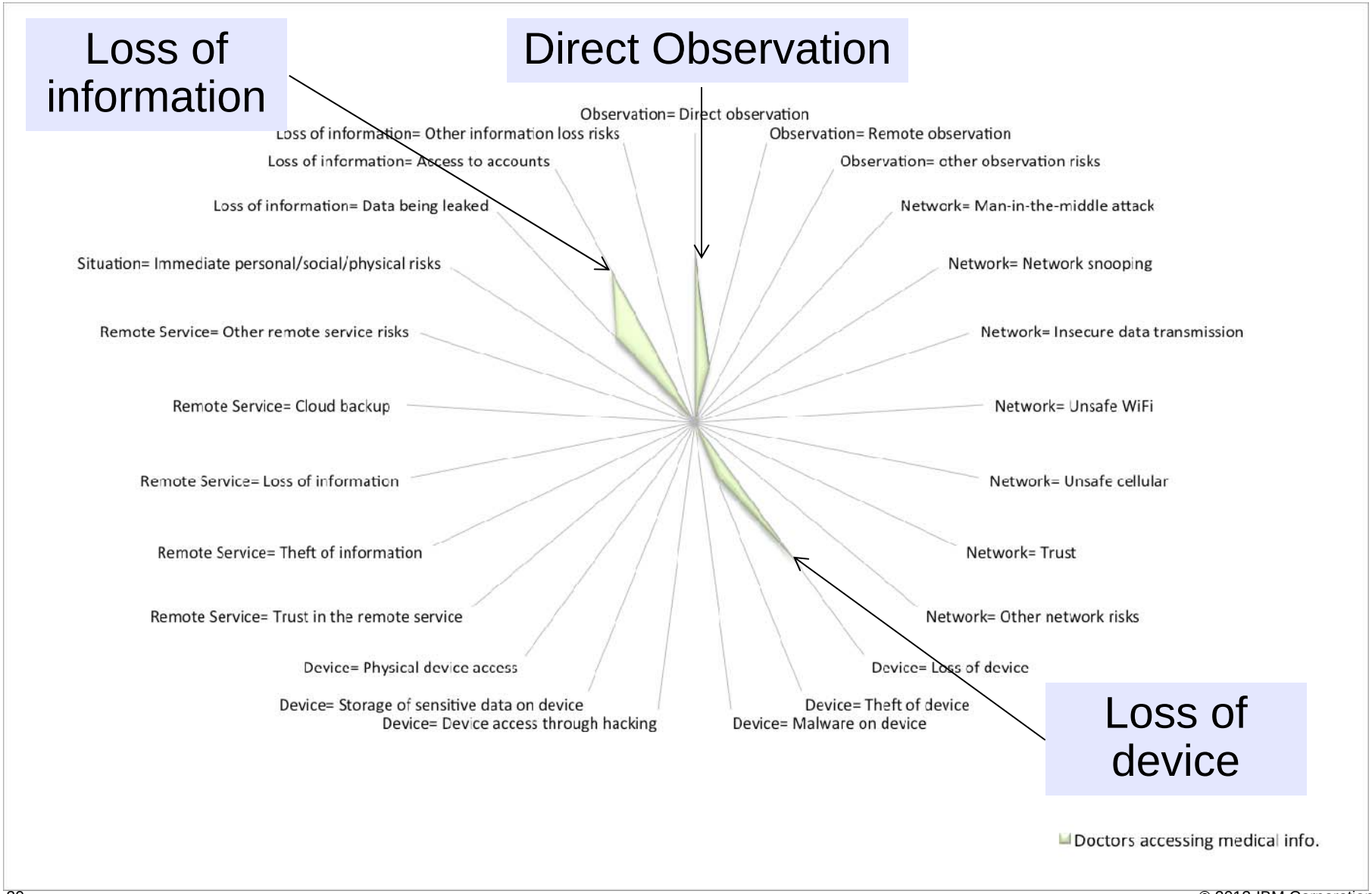
Perceived Risk - Risks perceived by IT Workers accessing company information



Perceived Risks –
Risks perceived in Personal Banking accessing financial information



Perceived Risk: Risks Perceived by Doctors Accessing Medical Information



Research Questions

1. Does the location have an effect on perceived information safety?
2. What risks do come to people's minds, when performing sensitive transactions on a mobile device?
3. What information do people use to decide whether it is safe?
4. What factors influence the decision to perform a sensitive transaction on a mobile device?

What information do people use to decide whether it is safe?

"What else would you want to know about these situations, to decide whether it is safe to access or enter sensitive information on your smartphone there?"

Information Wanted	IT	PB	D
Trust in the network connection	36	39	55
Trust in the remote service	30	37	0
Whether data is encrypted over the network	40	19	9
Possibility of being observed	17	0	18
Information about the situation	0	13	0
Security of the device	8	4	18
Legal recourse or protection	0	4	0
Value/sensitivity of information being accessed	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

Percentages of respondents from each group who wanted to know each kind of additional information, in order to decide whether to perform a mobile transaction

Experts Wanted to know

1. Who owns the network?
2. Is VPN being used?

Research Questions

1. Does the location have an effect on perceived information safety?
2. What risks do come to people's minds, when performing sensitive transactions on a mobile device?
3. What information do people use to decide whether it is safe?
4. What factors influence the decision to perform a sensitive transaction on a mobile device?

Factors Reported to Influence Decision

Factor	IT (%)	PB (%)	D (%)
Network risk	36	39	
Network protection	17	6	9
Observation risk	34	28	9
Time constraints	15	7	45
Sensitivity of data	15	7	
Physical location	13	26	
Digital device risk	11	17	
Need for the data	9	11	27
Physical device risk	9		
Magnitude of the Risk / Probability of data loss	8		18
Unknown retailer trust	6	15	n/a
Transaction time			27

Factors Reported to Influence Decision

Factor	IT (%)	PB (%)	D (%)
Network risk	36	39	
Network protection	17	6	9
Observation risk	34	28	9
Time constraints	15	7	45
Sensitivity of da	15	7	
Physical locatio	13	26	
Digital device risk	11	17	
Need for the data	9	11	27
Physical device risk	9		
Magnitude of the Risk / Probability of data loss	8		18
Unknown retailer trust	6	15	n/a
Transaction time			27

"can I enable VPN?", "approved company security protections in place"

Factors Reported to Influence Decision

Factor			D (%)
Network risk			
Network protection			9
Observation risk	34		9
Time constraints	15	7	45
Sensitivity of data	15	7	
Physical location	13	26	
Digital device risk	11	17	
Need for the data	9	11	27
Physical device risk	9		
Magnitude of the Risk / Probability of data loss	8		18
Unknown retailer trust	6	15	n/a
Transaction time			27

"Need access to critical test results anytime"

Factors Reported to Influence Decision

Factor	IT (%)	PB (%)	D (%)
Network risk	36	39	
Network protection	17	6	9
Observation risk	34	28	9
Time constraints	15	7	45
Sensitivity of data	15	7	
Physical location	13	26	
Digital device risk	11	17	
Need for the data	9	11	27
Physical device risk	9		
Magnitude of the Risk / P	8		18
Unknown retailer trust	6	15	n/a
Transaction time			27

"is the device free of viruses"

Factors Reported to Influence Decision

Factor	IT (%)	PB (%)	D (%)
Network risk	36	39	
Network protection	17	6	9
Observation risk	34	28	9
Time constraints	15	7	45
Sensitivity c	15	7	
Physical loc	13	26	
Digital devi	11	17	
Need for the data	9	11	27
Physical device risk	9		
Magnitude of the Risk / Probability of data loss	8		18
Unknown retailer trust	6	15	n/a
Transaction time			27

"How likely is it my device could be stolen while unlocked "

Factors Influencing Mobile Access Decisions – *"What factors affect your decision whether to access sensitive information in a given situation?"*

Experts considered the following three factors:

1. The consequences of the data being compromised
2. The urgency of the need to access the data
3. Whether they can protect the information (for example by hiding the screen from observers or cameras).

Discussion

- For many people, the dangers of mobile transactions do not easily come to mind.
  - Digital device security mentioned by < 15%.
  - Low concern about device theft or loss
- Perceived safety is affected by the close proximity of other people.
  - 2/3 are aware of this risk, but only 1/3 said it would influence their decision
  - Some users reported taking steps to reduce shoulder surfing risk
  - Seen as a controllable risk (more so than with laptop).
- People typically trust both app and web sites, in general, if they are familiar with the service provider.
- Trust in the network is a key factor in assessing risk.
  - Expertise affects what people want to know about the network
- Peoples' perception of risk does not extend to locking their mobile devices.
  - Difference in behavior between IT Worker vs. Personal Banking men.

Further Work

- Investigate actual decisions – potentially very different
- Explore contextual factors that impact perceived risk (people, network, personal safety, public access)
- Ask about real locations in each participant's life
- Explore personal safety, as opposed to information safety
- Other use cases may surface new risks
- How does this differ from laptop use?
- To what extent is behavior influenced by prior experience?

Summary

- We studied perceived information security risk for
  - IT Workers accessing company information
  - Personal banking consumers accessing their bank account, and
  - Doctors accessing medical records
- Location impacts perceived safety through the presence of potential observers, and through network security concerns.
- IT Workers had higher overall awareness of risk, and were more likely to lock their phones
- Information security risks did not easily come to mind in our scenarios, which may mean that people consistently underestimate the risks.

Related IT security work

- People believe they can protect against phone loss or theft, and it is unlikely to happen [Huang, Rau, Salvency, Shang, Lui, Wang, 2008]
- Online risks that can be related to known risks in the physical world are considered more serious [Garg & Camp, 2012]
- Non-experts may have a false sense of security in the setup of their home networks [Wash, 2010]
- Much security advice offers little benefit over the investment required to understand and act on it [Herley, 2009]
- People don't think they are likely to be victims of fraud, and don't feel responsible for negative outcomes [Davinson & Sillence]
- Online risk assessment (eg viruses, phishing, ID theft) is driven by familiarity of the risk and degree of dread [Garg & Camp '12]
- Willingness to perform sensitive activities on a phone vs. laptop [Chin, Felt, Sekar & Wagner '12]
  - Greater concern about smartphone as compared to laptop (network, no anti-virus, loss)
- Smartphone app risks [Felt, Egelman & Wagner '12]
  - Greater concern about apps with greater perceived impact (e.g., financial vs. social)
  - Age was a significant factor

Why look at risk perception?

- Willingness to perform security actions is a tradeoff between cost to the individual and perceived benefit [SBW01]
- Mismatch of perceived risk and system determined risk leads to poor user acceptance of technology [BSW08]
- Experts and non-experts respond differently [KST82]
- Experts use statistical reasoning to assess risk; non-experts rely on affect [ECH08]
- Characteristics that influence perception of risk [L76]:
  voluntariness, immediacy of effect, knowledge about the risk, available alternatives, and consequences