National Institute of Standards and Technology US Department of Commerce

Be Prepared: How US Government Experts Think About Cybersecurity

Mary Theofanos

Brian Stanton

Susanne Furman

Sandra Spickard Prettyman

Simson Garfinkel

NIST Previous Research in this Domain

- **General Public Research Results**
  - Finding 1:
    - Incomplete mental models
  - Finding 2:
    - Security fatigue
      - Resignation, loss of control, and frustration
  - Finding 3:
    - Leads to situations where the general public is unprepared

Next Phase of Research

- **Experts' Perceptions and Behaviors**
  - Highly specialized group of experts
  - Experts from three Federal Agencies
- **Definition of expert**
  - Qualifications and experience and what they do with those
    - Five years of experience
    - Inform policy and protect critical infrastructure

Next Phase of Research (cont.)

- **General Public Perceptions and Behaviors**
  - Considered to have less qualifications and experience
    - Do not work in the cybersecurity field
  - Use the internet and spend time online

Relevant Literature

- **Previous research in experts and non-experts has found:**
  - Utilize different mental models when thinking about computer and security risks (Asgharpour, et al. 2007)
  - Incomplete, oversimplified, and multiple mental models guide thinking and behavior (Camp 2009; Prettyman, et al 2015; Wash 2010)
  - Experts take different actions which result in different outcomes (Bravo-Lillo, et al 2011)
  - Experts and non-experts have different vocabulary and language (Stewart and Lacey 2012)
  - Expert and non-experts use different tools to protect themselves (Ion, et al 2015)

Methodology

- Research Questions:
  1. How do participants talk about their experiences with and perceptions about online privacy and security?
  2. If and what mental models guide participants' understandings, beliefs, and behaviors regarding online privacy and security?

- Qualitative Research that utilized in-depth interviews
  - Protocol development
  - Alignment matrix
    - Aligns research goals to interview questions
    - Provides consistency, logic, and transparency in the research process

- Interdisciplinary research team

Participants and Data Collection

	#	Gender		Age Range					
		M	F	18-20	21-29	30-39	40-49	50-59	60+
Experts	23	15	8	-	7	7	9	-	-
Non-Experts	21	9	12	3	7	4	2	2	3

- Expert interview times ranged from 17 to 55 minutes with an average of 32 minutes
- Non-Expert interview times ranged from 12 to 50 minutes with an average of 25 minutes
- All interviews were digitally recorded and transcribed verbatim

Data Analysis

- ***a Priori* Code List** (based on literature and our previous research)
  - Operationalization of all codes
  - All four researchers coded the first four interviews in each group
    - We chose not to calculate inter-rater reliability
    - "The degree of concordance between researchers is not really important; what is ultimately of value is the content of disagreements and the insights that discussion can provide for refining coding frames. The greatest potential of multiple coding lies in its capacity to furnish alternative interpretations." (Barbour, 2001)
- Code list revisions based on team discussions and emergent codes
- Iterative and recursive analytic process
  - Provided opportunities for interdisciplinary discussions and the development of alternative interpretations

Validity and Reliability

- In qualitative research referred to as trustworthiness, rigor, and quality
  - Trustworthiness:
    - well established research methods, triangulation, tactics to ensure honest responses, iterative questioning, frequent debriefing sessions
    - Use of participants' own words and ability to link back to data
  - Rigor – transparency and consistency in the research process and providing detail about all research processes

Limitations

- Focus solely on U.S. Government experts in Federal Agencies
- Non-Experts only come from D.C. Metropolitan area and the Midwest

Results – Three Themes

1) Experts did not seem to trust anything (anyone) in the online environment
2) The experts had all implemented plans to ward off or recover from risks they might encounter
3) Because the experts had plans in place to deal with any potential threat, they were not afraid

To Trust or Not to Trust

- Don’t trust: the lack of faith in individuals or systems to always act or perform in the expected way.
- Trust too much: the belief that individuals and the general public have too much faith in systems and technology which may put them or the systems at risk

Don’t Trust

- “Given what I know now, nothing has really made me feel 100% assured that anything is [safe] – whenever I go online I basically have to assume someone’s watching all the time.” (FedE:05 – 34:50)

- “I don’t think I ever feel safe online, it’s more of accepting risks. But it’s not safe because there’s so many ways that something can go wrong that are outside of my control.” (FedE:13 – 20:42)

- “So I think my answer to that would be never [in response to the questions – do you feel safe online?]. I am not saying there won’t come a time when people could be made safer online, sure I would be open to that. But right now it’s almost like a dream.” (FedE:05 – 34:50)

Trust Too Much

- "I think people tend to be gullible. They believe what they see. If you find it on a document on the internet it has to be true." (FedE:06 – 19:15)

- "Yeah, I think for me there is a lot of trust that isn't always probably, properly earned. You know, I don't read through the PayPal stuff because it's a big – I trust that and I trust that Amazon or any number of Websites are not either going to sell my information or they will protect it." (MWGP:05 - 2:51)

- "I guess I'm going with the whole, "oh well, everybody else was okay, so I'll be okay too," just hope for the best." (MWGP:09 – 9:53)

To Plan or Not to Plan – Experts Plan

- Experts took a risk-based approach to cybersecurity where they saw risk everywhere and therefore need to use cybersecurity tools to protect themselves.

- Proactive definition: Protection and/or a plan against potential consequences before they happen.

- “I think I’m pretty aware of my environment, so I have adopted a set of best practices. I would say, about interacting with the technology. So I think I tend to have the right kind of measure for whatever I do.” (FedE:04 – 10:32)

- “I work with security people, so we take all kinds of precautions, but the average person … I don’t think they take enough precautions.” (FedE:18 – 13:20)

To Plan or Not to Plan – Non-Experts Don’t Plan

- Non-experts took an avoidance-based approach, either relying on the people and sites they interacted with to protect them or believing they had nothing of value and did not have to worry about security.
- Reactive definition: Response to something that happened.
- No, I think I will be reactionary and not proactive. I think that if something happens, if something bad were to happen, then I would be the type of person to change all my passwords… but I’m not proactive about my own security, I’m much more reactive.” (MWGP:02 – 19:32)
- “I honestly don’t know much about online security. I don’t know how that works at all. I really don’t so it’s sometimes uncomfortable for me… You know how I feel about security is that avoidance means it’s going to go away. That’s pretty much how I deal with it” (MWGP:01 – 2:13)

To Fear or Not to Fear

- We coded fear as an emotion: an emotional reaction based on the belief that someone or something was a threat or was potentially dangerous.
- Instead of fear, many experts felt a sense of excitement when thinking about cybersecurity or weren't worried. But also frustration.
- "I basically assume that my technical skills will help me to recover from anything that might happen, and I take reasonable steps to protect my computer and myself. But I don't worry about it too much, suck the joy out of life. Right? (FedE:11 – 10:46)
- "There's excitement on my end, because there's so much to learn. It's crazy…. There's learning for the sake of learning – you can work with some cutting edge technologies on some very sophisticated stuff." (FedE:18 – 22:43)
- "I guess it's just sometimes you get frustrated with people that aren't taking it seriously… If they haven't followed the procedures that they need to." (FedE:19 – 8:19).

To Fear or Not to Fear – Non-Experts

- Non-experts often expressed very different emotions when talking about the risks they faced.
- They used words as: uncomfortable, fear, helplessness, anxiety, worry, afraid, and confusion.
- "There's always going to be a small sense of worry so there's always that sense of worry when you see things in the news, and when small things happen to you." (DCGP:02 – 9:59)
- "I guess fear I think would be the big one [when asked what emotions they feel about online privacy and security]." (MWGP:05 – 16:24)
- "Maybe anxiety or fear that I could be taken advantage of in some way." (MWGP:06 – 9:49)

Conclusions

- U.S. Government experts think and behave differently about cybersecurity than the non-experts we interviewed
- Government experts have a solid base of knowledge, therefore they are less trusting, which leads to putting plans in place, making them proactive which leads to them having less fear.
- Non-experts have less knowledge which often leads to them trusting too much as a result they do not put plans in place, and tend to be reactive.
- Non-experts need a plan that is contextualized and individualized that becomes a habit
- Everyone needs to be prepared! And that must become a habit.

Future Research

- Expand to other demographics and populations
- Look more specifically at being prepared
- Relationship between security fatigue, habit and being prepared

Thank You

Contact Susanne.furman@nist.gov

Questions