“It’s Scary...It’s Confusing...It’s Dull”: How Cybersecurity Advocates Overcome Negative Perceptions of Security

Julie Haney
Visualization & Usability Group
National Institute of Standards and Technology
FISSEA 2019 - June 27, 2019
Motivation

Cyber attacks are on the rise, but people often fail to adopt and effectively use security best practices and technologies.

"From the audience’s perspective, security can be characterized by three major factors: one, it’s scary; two, it’s confusing; three, it’s dull."

--P08
Cybersecurity Advocates

- **Cybersecurity advocates** are security professionals who promote and encourage security adoption as a major component of their job.

- Examples:
  - Security awareness professionals
  - Secure development champions
  - Security consultants
  - Non-profit security advocacy staff

- Must be effective at communicating security risk, motivating behavior change, and overcoming negative perceptions of security.
Research Questions

• What are the professional characteristics and skills that cybersecurity advocates employ in their work?

• What techniques do cybersecurity advocates use to encourage security adoption?
Research Study

• Interviewed 28 cybersecurity advocates
  • 10 females, 18 males
  • Various job roles – e.g., consultants, security engineers, security awareness professionals, educators
  • Diverse educational backgrounds – 14 with at least one non-tech degree
  • Experienced group – most > 10 years experience in security
  • Multiple sectors - industry, government, higher education, non-profits
  • Diverse audiences – internal and external

• Questions on work practices, professional motivations, challenges, characteristics of successful advocates
Establishing Trust

"Trust is the most important thing that I have."

-- P12
Demonstrating Technical Knowledge

You really do need to understand the technology...This stuff’s tricky, and you don’t just guess your way out of it.

-- P08
I think people have to have a **high emotional intelligence** and especially **empathy**. Part of being successful in this is being able to have a conversation and put yourself in the place of the person that you’re working with, and then be able to give effective advice that is not preaching, is trying to be helpful, and is letting them know that they’re not stupid because they may not know how to do certain things.

-- P18
Overcoming “It’s Scary”

“... We’re just really a fear-mongering industry.”

-- P21
You can’t appreciate the importance of security without first understanding what’s at stake, what’s at risk.

-- P14

If I told everyone what I know, they’d freak out. I want to tell a smaller list of people I know so that we can quietly fix it.

-- P11
Empowerment

I love empowering people and seeing their lightbulbs go off in the moment that they understand why they are a target and what they can do about it. So, it’s not a place of fear. You have to start with fear to get them to understand that there’s a problem, but then you also give them the tools.

--P21
Overcoming “It’s Confusing”

“Security is mysterious to most people.”  
-- P07
Bridging the Gap: Translation & Context Awareness

Being able to translate complicated things very simply is crucial...

-- P02

You have to assimilate to and acclimate to the language and the beliefs and the culture that you are trying to affect.

-- P11
Providing Practical Recommendations

I think in the security area there’s a lot of mythology and a lot of things we do because we heard it’s the right thing to do. And we have no idea why, but everybody else seems to be doing it, so we should do it, too. And so, trying to get people to stop and think it through, and figure out what’s actually going to be effective.

--P07
Overcoming “It’s Dull”

“Nobody wants to spend their time doing security.”

-- P07
I am trying to drive them to make themselves more secure by using various argumentative techniques. And, in some way, that’s manipulating them. But if you’re manipulating somebody for their own good, that’s not wrong.

--P10
Using Engaging Communication Techniques

You can feel the energy that they believe in it.
-- P14

Personalizing the message is useful, seeing that this happens to real people.
-- P07
Takeaways

• Advancing risk communication
  • Relationship to non-security risk domains
  • Strategies for communicating security risk

• Emerging cybersecurity advocate role
  • Continuing education efforts to support progression from other roles and disciplines
Current/Future Efforts

Cybersecurity Advocacy in Practice

• In progress: Case study of a security awareness team/program at a federal agency

• Future: Collect lessons learned and success stories from other federal agencies
Related Papers


julie.haney@nist.gov

NIST Usable Cybersecurity
https://csrc.nist.gov/Projects/Usable-Cybersecurity