The Role of Education in Dispelling Myths and Misconceptions in Cybersecurity

Eugene H. Spafford, Leigh Metcalf, Josiah Dykstra

This Panel

Our basic themes:

- Cybersecurity is not simply about technology, and never really has been. (Spafford presented a keynote on exactly this topic in 2000 at this conference.). It has a large component in people–their perceptions, actions, structures, and policies.
- People are not perfected automata – they have built-in biases, hold misconceptions, develop myths, and make mistakes. These should be addressed, too.

Agenda

- Some examples
- Worked curricula
- Your questions

Leigh Metcalf

Leigh Metcalf is a Senior Network Security Research Analyst at the Carnegie Mellon University Software Engineering Institute's cybersecurity (CERT) division. CERT is composed of a diverse group of researchers, software engineers, and security analysts who are developing cutting-edge information and training to improve the practice of cybersecurity. Before joining CERT, Leigh spent more than 10 years in industry working as a systems engineer, architect, and security specialist.

Dr. Metcalf has presented research at numerous conferences. She is the co-author (with William Casey) of the book Cybersecurity and Applied Mathematics (Syngress, 2016) as well as the co-author (with Jonathan Spring) of the book Using Science in Cybersecurity (World Scientific, 2021). She is also the Co-Editor-in-Chief (with Arun Lakhotia) of the ACM journal Digital Threats: Research and Practice (DTRAP).

There is a great misunderstanding of statistics, what they tell you, and what they can mean. Statistics don't exist in a vacuum—the context matters. Understanding that helps people understand the numbers that statistics provides us and helps us make better decisions.

Josiah Dykstra

Josiah is a seasoned cybersecurity practitioner, researcher, author, and speaker. He is a senior leader in the Cybersecurity Collaboration Center at the National Security Agency (NSA) and the owner of Designer Security, LLC. Dr. Dykstra holds a Ph.D. in computer science and previously served as a cyber operator and researcher. He is interested in cybersecurity science, especially where humans intersect with technology. He has studied stress in hacking, action bias in incident response, and the economics of knowing when sharing threat intelligence is more work than it is worth.

Dr. Dykstra is a frequent author and speaker, including Black Hat and RSA Conference. He received the CyberCorps ® Scholarship for Service (SFS) fellowship and is one of six people in the SFS Hall of Fame. In 2017, he received the Presidential Early Career Award for Scientists and Engineers (PECASE) from then President Barack Obama. Dr. Dykstra is a Fellow of the American Academy of Forensic Sciences and a Distinguished Member of the Association for Computing Machinery (ACM). He is the author of numerous research papers and the book Essential Cybersecurity Science (O'Reilly Media, 2016). More information may be found at https://josiahdykstra.com

I've seen a recurring misconception that people would be more protected by simply sharing more. This builds on a misconception that sharing is cheap/free. There is research that tries to fix the logistical mechanisms of sharing but that's not the whole problem. How do we evaluate the quality and value of CTI? This myth is related to others, including how difficult it is to measure security outcomes (i.e., success is not the quantity of sharing).

At Purdue

- Background: Interdisciplinary Information Security Graduate Program (INSC)
  - Started in 2000
  - Requires a class in technology policy
  - Requires a class in technology ethics
  - Encourages a class in experimental statistics

CS 523 (Grad)

Topics:

- Basic economics
- Risk
- Human Biases
  - Cognitive
  - Discrimination
- Common misconceptions
- Legal issues
  - Civil
  - Criminal
- Cyberwar
- International norms

CS 390 (undergrad)

Topics:

- Human Biases
  - Cognitive
  - Discrimination
- Common misconceptions
- Legal issues
  - Civil
  - Criminal
- Privacy
- Issues related to AI and ML
- International norms

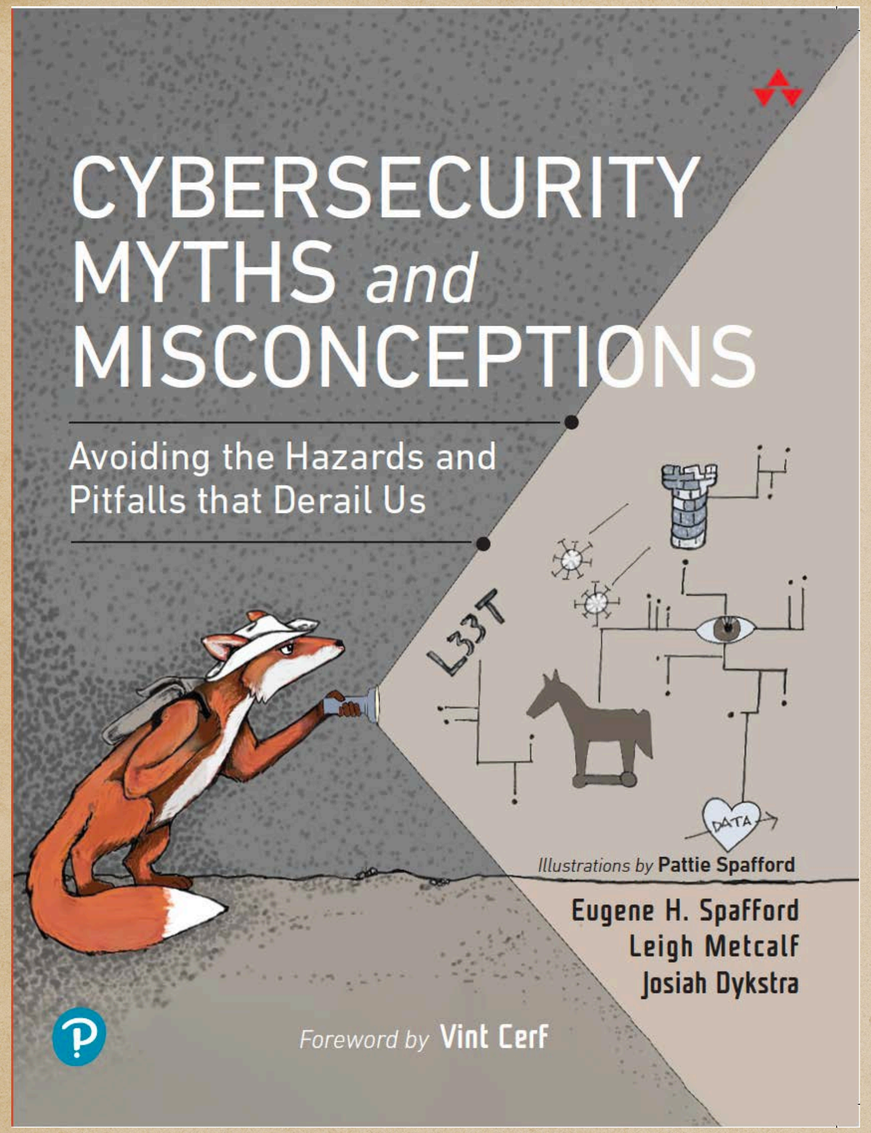
Common Issues

Topics:

- Human Biases
  - Cognitive
  - Discrimination
- Common misconceptions
- Legal issues
  - Civil
  - Criminal
  - Cyberwar
- International norms

Contextual Topics

- What is Cybersecurity?
- What is the Internet?
- How do myths arise?
- Logical fallacies
- Basic Statistics
- Perceptual Limitations
- Misuse of analogies



Visit

https://cybermyths.info

for more information

(Depending on your browser this may generate a warning about certificate/ domain. You can ignore this.)

Questions? Comments?