

Article: Comprehending Cybersecurity via Interdisciplinary Frameworks: A Sociocultural Perspective

Article: <https://academic.oup.com/cybersecurity/pages/About>

Cybersecurity is closely related to the social sciences because it protects data and information in a world that is becoming more digital and linked. To understand the human side of cybersecurity, you need to know about things like human behavior, social relationships, and cultural norms. Psychological and sociological factors affect how people act online, how much they trust digital platforms, and how easily they can be tricked by cyber risks like phishing and social engineering. Another important thing to think about when trying to solve cybersecurity problems is how different social groups interact with technology. This could be because of differences in income or access to digital tools.

The journal makes a point of saying that cybersecurity isn't just about computer science, but also about knowing how people think, feel, and interact with each other. It fits with the social sciences, which look at how people, groups, and processes in society interact with each other. Because of this, a multidisciplinary approach to cybersecurity needs to take into account social factors like trust, privacy, and social values, which all have a big impact on how well cybersecurity works.

Questions and ideas for research

Many of the studies in the Journal of Cybersecurity are based on research questions that look at more than just the technical side of security systems. These questions also look at human, cultural, and organizational aspects. Some of these questions could be:

1. How do different cultural views on privacy and trust affect how widely cybersecurity methods are used and how well they work?
2. What psychological factors affect how people react to cyber risks like identity theft or social engineering?
3. What are the connections between cybersecurity policies and practices and social justice problems, especially when it comes to communities that aren't getting enough help or are on the outside?

Some studies might suggest that cultural values, socioeconomic position, or education level affect how people in different social groups think about and act on cybersecurity. The goal of these theories is to find out how these social factors affect technical measures of cybersecurity, resulting in different levels of vulnerability and security behaviors.

How to Do Research and How to Look at Data

According to the Journal of Cybersecurity, research in the area of cybersecurity often uses both qualitative and quantitative methods to look at both the technical and human sides of the subject. Like this:

1. Polls and Talks: A lot of studies poll people or talk to groups to get more in-depth information about how they feel about cybersecurity laws, how they feel about online privacy, or their experiences with cyber threats. These methods help experts learn about the things that people do that affect cybersecurity, like trust, fear, and gaps in knowledge.
2. Case Studies: One way to look at cybersecurity is through the lens of how certain groups (like small businesses, disadvantaged individuals, or emerging countries) use it. In the real world, these case studies can give you a lot of useful information about the difficulties of keeping your computer safe.
3. Statistical Analysis: To do statistical analysis, quantitative researchers often use data from security incidents, breach reports, or cybercrime figures. Researchers can find weaknesses and patterns that help make security better by looking at how cybersecurity incidents happen in different areas, among different groups of people, or within different types of companies.
4. The field of human-computer interaction (HCI) studies how people use security systems, websites, and apps. HCI methods are used to look at user behavior. By watching how people use a product, experts can figure out how mistakes in the design or problems with how it's used could cause security problems, like weak passwords or sharing private data without meaning to.

Facts and Figures

1. Incident Reports: Information about cyberattacks, data breaches, or identity theft is looked at to find trends in attack vectors, target groups, and security holes.
2. Surveys of Cybersecurity Awareness: These polls find out what people know and how they feel about cybersecurity issues, like how well they understand phishing attacks, how to handle passwords, and the dangers of public Wi-Fi.
3. As social media plays a bigger part in cyber threats (like social engineering attacks), some studies look at how people use social networks to see how their public posting habits might accidentally reveal personal information or give hackers a way to get into computers.

Looking for trends, correlations, or causal relationships between things like level of education, income, social media use, or past experience with cyber threats and the chance of being attacked or becoming a victim of cybercrime is a common way to look at this data.

Relevance to ideas from the PowerPoint videos

According to the magazine, the study of cybersecurity has a lot in common with ideas that are talked about in cross-disciplinary classes or presentations about the social sciences. Like this:

1. **Social Class and Access to Technology:** People from underrepresented groups may have a harder time getting cybersecurity schooling or technology, which makes them more likely to be victims of cybercrime. Figuring out these differences is important for dealing with the social parts of cybersecurity.
2. **The study of human psychology,** like how people make decisions when they don't know what to do or how to assess risk, is very important for understanding how people and businesses make choices about cybersecurity. Psychology and sociology have ideas about how people judge danger, trust technology, and respond to security breaches that are similar to these ideas.
3. **An important problem in cybersecurity is privacy,** which is also at the heart of many debates in the social sciences. The study of how different groups and cultures define and protect privacy helps connect technical security measures with bigger issues of fairness and ethics.

Connection to the Problems and Helps of Groups that are left out

How policies and practices in cybersecurity affect groups that are already at a disadvantage is one of the most important topics of multidisciplinary cybersecurity study. Like this:

1. **Digital Divide:** People in low-income areas, rural areas, or racial or ethnic groups that aren't well-represented may not have easy access to technology and cybersecurity tools, making them more likely to be attacked online.
2. **Cybercrime Victimization:** Cybercriminals may target older adults or people who don't know how to use technology well more than other people. To make better, more inclusive cybersecurity laws, we need to know how cyberbullying, identity theft, and scams affect these groups.
3. **Privacy Concerns:** Underprivileged groups, especially in authoritarian regimes or areas with low incomes, may be more likely to have their privacy invaded by things like government spying or companies collecting personal information. This makes protecting privacy a very important problem.

Contributions to society as a whole

The study published in the Journal of Cybersecurity makes a big difference in the world because it shows that cybersecurity isn't just a technical problem but a complex one with social, cultural, and political aspects. The multidisciplinary approach helps us learn more about:

1. How people's minds affect security choices and the ways that people are weak in the digital world.
2. There are differences in how people from different cultures think about and use cybersecurity, which can help make security solutions more effective for all kinds of people.
3. Cybercrime's effects on society and the economy, especially on underrepresented groups, and how policy and education can help lessen these effects.
4. By looking at the social and human parts of cybersecurity, the journal encourages solutions that work for everyone. This makes sure that everyone has equal access to digital safety and protection, which is good for everyone.

Conclusion

The Journal of Cybersecurity encourages a multidisciplinary approach that shows how different fields need to work together to solve the many problems that come up in cybersecurity. Focusing on human factors, social problems, and the experiences of disadvantaged groups in the journal gives readers a deeper understanding of cybersecurity than solutions that are only technical. People and businesses are safer thanks to these studies, and everyone can enjoy the benefits of digital technology fairly.