Teaching Social Science Aspects of Information Security

Igor Bernik
Faculty of Criminal Justice and Security, University of Maribor, Slovenia

igor.bernik@um.si

Abstract: As information security has become increasingly crucial in our daily lives, there is a growing need to teach its social science aspects. This paper explores the challenges and best practices for teaching social science aspects of information security. It begins with the importance of information security and cyberspace and highlights the human aspects of information security. Next, it discusses the role of social science in understanding information security and how social science can help us better design and implement security measures. The paper identifies challenges in teaching social science aspects of information security, such as the interdisciplinary nature of the subject and the need for a standardised curriculum. Finally, the paper outlines best practices for teaching social science aspects of information security, such as using case studies and real-world examples, incorporating interactive and experiential learning, and leveraging existing resources. The conclusion highlights the importance of incorporating social science aspects of information security in education and suggests future research directions.

Keywords: Information Security, Cyberspace, Social Science, Human Aspects, Teaching

1. Introduction

In recent years, the importance of social science in information security education has become increasingly recognised. Information security is a complex field involving technical aspects and social and human factors (Moor, 2010; Singh et al, 2018). Several researchers have noted that human factors are crucial in information security, including how people interact with information systems (Kumar and Pang, 2015; Mitropoulos et al, 2018). Understanding the human factors contributing to security incidents is critical to developing effective solutions. Social science can help us better understand the human aspects of security, including the motivations and behaviours of attackers, the psychology of users and employees, and the cultural and organisational factors that influence security (Furnell and Warren, 2015; Mitropoulos et al, 2018). Human factors are influenced by the broader socio-technical context in which information systems operate (Clarke, 2014; Moor, 2010). This context includes organisational culture, social norms, and legal and regulatory frameworks. Therefore, effective information security requires technical solutions and consideration of these broader contextual factors.

At the Faculty of Criminal Justice and Security at the University of Maribor (UM FCJS), we have offered an undergraduate Information Security program since 2010. In addition to the essential technical aspects, our program focuses mainly on the sociological and criminological aspects of information security. Given the nature of the teaching of security studies at the time, we decided that our program would be different from most of the available programs and would focus not only on the technical but also on the security and social sciences aspects of information security, preparing students for the constantly changing technologies and the associated security issues in cyberspace. Therefore, we have provided the following definition of information security: "Information security is an interdisciplinary field that studies phenomena from the perspective of computer science, information systems, security studies, internal security and protection, develops and studies mechanisms that society uses to ensure security and privacy, and the protection of the state, ensuring security in the community, organisations, and individuals against behaviour that may harm the individual, community, or state, and develops theories and methods for protecting the information and privacy of the subjects as mentioned above." (UM FCJS, n.d.) The curriculum, in addition to the basic methodological and technical knowledge of information systems and information security, includes areas of (criminal, procedural, and administrative) law and government regulation, national security, management and administration, sociology, psychology, criminology, and criminality. Over the decade of implementation and changes to the program due to technological advancements and constantly evolving needs in the economy, we increasingly find that the sociological aspects of information security are equally important as the technical aspects. Based on our experience and literature studies, we provide some guidelines for preparing information security content and study programs that move away from traditional technical fields and towards security studies and management.

Social science can help us better understand the human aspects of security, including the motivations and behaviours of attackers, the psychology of users and employees, and the cultural and organisational factors that influence security (Gordon et al, 2017). With the research on vulnerabilities in information, systems were identified to understand how people interact with technology and develop more effective security policies and practices (Bada and Sasse, 2014). For example, social science research has shown that users often struggle to

understand complex security warnings and are likelier to click phishing links when distracted or under stress (Kumaraguru et al, 2013). This knowledge can inform the design of more user-friendly security interfaces and better security awareness training. Security decisions can significantly impact individuals, organisations, and society, and it is essential to consider these impacts. Social science research can help us to understand the trade-offs between security, privacy, and other values and to develop security policies that balance these competing interests (Van den Berghe and Walgrave, 2016). Including social science subjects in information security education can help students develop a more holistic and nuanced understanding of security and develop the critical thinking and problem-solving skills needed to address the complex security challenges of the future.

This paper explores the social science aspects of information security and provides educators with practices and strategies for teaching these aspects in their curriculum. It will also discuss educators' challenges in teaching social science aspects and offer suggestions for future research and improvement in information security education.

2. Understanding Social Science in Information Security

Social science aspects of information security refer to the broader socio-technical context in which information systems are situated, including the human and social factors that influence the security of information systems (Furnell and Warren, 2015). Factors include the human behaviours, attitudes, and motivations of individuals and groups, as well as the cultural and organisational context in which they operate:

1. Human behaviours: This factor refers to the actions that individuals take in their interactions with information systems, such as their adherence to security policies, their password management practices, and their use of personal devices for work purposes. Research (Kumar and Pang, 2015) has shown that human error is a major cause of information security incidents, making it crucial to understand and address human behaviours in information security.
2. Attitudes: Attitudes refer to individuals' beliefs and feelings about information security, including their perceived risks, trust in the system, and willingness to comply with security policies. Understanding individuals' attitudes can help organisations design effective security awareness training and communication strategies (Van Niekerk and Von Solms, 2017).
3. Motivations: Factor refers to why individuals may engage in risky behaviours, such as hacking or sharing sensitive information. Motivations can be influenced by financial gain, revenge, or a desire for recognition (Singer and Friedman, 2017). Understanding these motivations can help organisations design effective deterrence strategies and address underlying vulnerabilities.
4. Cultural context: Culture refers to the shared values, beliefs, and norms that shape individuals' behaviours and attitudes. Cultural factors can influence how individuals perceive and respond to security threats and shape organisational practices and policies (Singh et al, 2018). Understanding cultural factors is essential for designing effective security strategies in diverse settings.
5. Organisational context: This factor refers to the policies, procedures, and structures that shape how individuals interact with information systems within an organisation. Organisational context can influence the effectiveness of security controls and the willingness of employees to comply with security policies (Mangalaraj et al, 2016). Understanding the organisational context is essential for designing effective security policies and practices.

While technical solutions and tools are important in securing information systems, understanding the social and human factors that influence security is equally important. Social science research can help us better understand individuals' and groups' behaviours, motivations, and attitudes concerning information security and develop more effective policies and practices to improve safety and security.

3. Challenges in Teaching Social Science Aspects of Information Security

Teaching social science aspects of information security can be challenging for educators, as it requires them to address complex and multifaceted issues beyond purely technical concerns. Here are some of the challenges that educators may face:

1. Interdisciplinary nature: Social science aspects of information security draw on various disciplines, including security, psychology, sociology, and law. Educators may need a broad knowledge (Furnell and Warren, 2015; Singh et al, 2018) to teach social science aspects of information security effectively.

2. Lack of integration: Social science aspects of information security may not be well integrated into existing information security curricula. Educators may need to develop or modify new courses to address mentioned topics (Clarke, 2014; Mitropoulos et al, 2018).
3. Difficulties in measurement: Social science research often involves qualitative or subjective data, which can be more difficult to measure than quantitative data. This can make it challenging for educators to assess student learning and evaluate teaching methods' effectiveness (Furnell and Warren, 2015).
4. Limited resources: Educators may need more resources (Furnell and Warren, 2015; Mitropoulos et al, 2018), such as time, funding, or access to social science experts, to develop and implement effective teaching strategies.
5. Resistance to change: Educators may encounter resistance (Singh et al, 2018; Mitropoulos et al, 2018) from students and/or other stakeholders who are more focused on technical aspects of information security and may not see the value of social science approaches.
6. Rapidly evolving field: Social science aspects of information security are constantly changing as new technologies and threats emerge. Educators must stay up-to-date with the latest research and developments (Furnell and Warren, 2015; Clarke, 2014) to teach relevant and timely information.

Addressing these challenges requires educators to be creative, flexible, and collaborative. They may need to collaborate with social science experts and other educators to develop effective teaching strategies and to advocate for the importance of social science aspects of information security within their institutions and the broader community. Ways to overcome the mentioned challenges faced by educators:

1. Collaboration: Educators can collaborate with social science experts and other educators to develop interdisciplinary approaches to teaching social science aspects of information security. By working together, educators can leverage the strengths of each discipline and create more comprehensive and effective teaching strategies.
2. Integration: Social science aspects of information security can be integrated into existing information security curricula. This can involve modifying existing courses or developing new ones incorporating social science topics. Educators can also use case studies and examples that illustrate the relevance of social science to information security.
3. Active learning: Social science aspects of information security can be taught through active learning approaches that engage students in problem-solving and critical thinking. For example, educators can use group discussions, debates, and simulations that challenge students to analyse complex issues and make informed decisions.
4. Assessment: Educators can use various assessment methods to measure student learning, including written assignments, presentations, and practical exercises. Rubrics and clear learning objectives can help educators assess student learning outcomes and identify areas for improvement.
5. Professional development: Educators can stay up-to-date with the latest research and developments in social science aspects of information security by attending conferences, workshops, and webinars. Professional development opportunities can also help educators develop new teaching strategies and connect with peers in the field.
6. Advocacy: Educators can advocate for the importance of social science aspects of information security within their institutions and the broader community. This can involve engaging with decision-makers and stakeholders, highlighting the relevance of social science to information security, and showcasing examples of successful teaching strategies.

Above are strategies that educators can use to overcome these challenges and effectively teach the social science aspects of information security. Collaboration with social science and information security experts can help educators bring a deeper understanding of the social science aspects of information security into the classroom. Integrating social science topics into existing curricula can make the material more accessible and relevant to students. Active learning approaches, such as case studies and role-playing exercises, can engage students and help them apply social science concepts to real-world scenarios. Effective assessment methods can evaluate students' understanding of social science concepts and skills. Finally, ongoing professional development and advocacy for the importance of social science in information security can help educators stay current with the latest research and trends in the field.

Research in the field of education and information security supports these strategies. For example, a study by Maguire et al (2020) found that integrating social science topics into a cybersecurity curriculum increased students' interest in the subject and improved their critical thinking skills. Similarly, a study by Olson and Yousuf (2019) found that active learning approaches, such as problem-based learning and role-playing exercises,

improved students' understanding of social science concepts in information security. Teaching the social science aspects of information security is crucial for preparing students to address the complex challenges of the field.

4. Best Practices for Teaching Social Science Aspects of Information Security

Teaching information security requires a nuanced understanding of technical and social science aspects. However, educators need help effectively teaching the social science aspects of information security. To overcome the above challenges, there are presented best practices that educators can implement to effectively teach the social science aspects of information security. Effective teaching methods and strategies for teaching social science aspects of information security are:

1. Active learning: Active learning approaches, such as group discussions, problem-based learning, and case studies, effectively teach social science aspects of information security (Jøsang, 2017; Kim and Kim, 2019). These methods engage students in critical thinking and problem-solving and help them to apply social science concepts to real-world situations.
2. Multidisciplinary approaches: Social science aspects of information security require a multidisciplinary approach that draws on multiple disciplines, including psychology, sociology, anthropology, and law (Siponen, Vance and Willison, 2018). Educators can use multidisciplinary techniques to create more comprehensive and effective teaching strategies.
3. Experiential learning: Experiential learning approaches, such as internships, co-op programs, and service-learning projects, teach social science aspects of information security (Morrow and Brown, 2015). These methods provide students with hands-on experience and allow them to apply social science concepts in real-world settings.
4. Technology-enhanced learning: Technology-enhanced learning approaches, such as online courses, simulations, and virtual reality environments, effectively teach social science aspects of information security (Martin, 2017; Siponen et al, 2018). These methods provide students with flexible and interactive learning opportunities that can simulate real-world scenarios.

With the teaching methods and strategies, educators can effectively teach these topics and prepare students for a career in information security. With a deeper understanding of the social science aspects of information security, students can become well-rounded professionals equipped to address the complex challenges of the field. We can effectively integrate social science into the information security curriculum by employing methods and strategies. This integration provides students with a comprehensive understanding of the diverse and multifaceted nature of information security, enabling them to address the complex challenges of the field and contribute to the development of sustainable security solutions. Social science provides students with the tools and knowledge to analyse and manage these factors, including the psychology of cyber attackers, the impact of social norms and culture on security practices, and the ethical and legal implications of information security decisions. By integrating social science into the information security curriculum, students are better prepared to tackle the real-world challenges of the field and contribute to the development of effective and sustainable security solutions.

While there are various approaches to improving curricula, we recommend the following steps based on their proven success in practice:

1. Identify social science topics: The first step is identifying topics relevant to information security. These topics include human behaviour, ethics, psychology, organisational culture, and risk management.
2. Incorporate social science topics into existing courses: Social science topics can be integrated into existing information security courses, such as new technologies (artificial intelligence, Big Data etc.), network security, cybercrime and cyber warfare, crisis management and similar. For example, students could be asked to analyse the psychological motivations behind cybercriminal behaviour or to develop risk management strategies based on organisational culture.
3. Develop new courses: Institutions can also develop new courses that specifically focus on the modern aspects of information security. These courses could cover cybersecurity ethics, social engineering, and risk perception.
4. Partner with social science departments: Collaboration with social science departments can be beneficial in integrating social science into the information security curriculum. Joint courses or interdisciplinary projects can give students a more comprehensive understanding of information security.

At UM FCJS, we have successfully upgraded the curriculum by incorporating the presented teaching methods and strategies, allowing us to meet employers' demands. Our undergraduates' Information security program offers students a contemporary and exciting course of study that equips them with the knowledge necessary for success in their career development. As we move forward, we remain committed to further enhancing the program in line with the evolving trends and guidelines of the field. As a result, our graduates are highly sought after as experts and are recognised for their vital contribution to establishing contemporary business practices within their respective organisations.

5. Conclusion

The integration of social science aspects into information security education is crucial for producing well-rounded professionals who understand the human aspects of cybersecurity. By incorporating social science topics (Whitman and Mattord, 2016, Herath and Rao, 2019), such as human behaviour, ethics, psychology, organisational culture, and risk management, into the curriculum, educators can help students develop a more comprehensive understanding of information security. Educators need to work on teaching social science aspects of information security, such as the lack of interdisciplinary expertise, difficulty keeping up with rapidly evolving technologies, and students' reluctance to engage with social science topics (O'Connor and Lada, 2018). Several best practices can be used to overcome these challenges, such as active learning strategies, collaboration with social science departments, and real-world case studies (O'Connor and Lada, 2018). One of the examples is the introduction of database content as a technical element of information security, where data is also defined with a sociological and behavioural approach and understanding so that students understand the mathematical and technical connections between data and the impact of these on behaviour, perception and response of the individual dealing and working with data. Such an approach is geared towards enhancing students' understanding of this field.

Future research will focus on evaluating the effectiveness of these best practices in teaching social science aspects of information security, developing new interdisciplinary teaching methods, and exploring how emerging technologies such as artificial intelligence and blockchain can be integrated with social science topics. The focus would help create a more well-rounded and comprehensive curriculum that accounts for cybersecurity's social and technological aspects. Future research in these areas can further improve the quality of information security education and better prepare students for the complex security challenges of the future.

The importance of social science in information security education must be considered. By providing insights into the human factors that impact security and the broader societal implications of security decisions, social science can help to develop more effective security policies and practices. Educators can overcome the challenges of teaching social science aspects of information security by using effective teaching methods and strategies and integrating social science topics into the curriculum.

Acknowledgements

This publication is part of the Green and Resilient Transition for a Safe and Successful Society project, co-financed by the Ministry of Higher Education, Science, and Innovation of the Republic of Slovenia and the European Union's NextGenerationEU initiative.

References

Bada, M., and Sasse, M. A. (2014). *Research into usable security: Where are we now, and where do we go from here?* Proceedings of the 28th International BCS Human Computer Interaction Conference, pp 1-10.

Clarke, R. (2014). *Social issues and security. In Computer security, privacy and politics: Current issues, challenges and solutions* (pp 19-36). Springer International Publishing.

Furnell, S., and Warren, M. (2015). *Human factors in security. Cyber security: Management, systems, governance and assurance* (pp 127-146). Springer International Publishing.

Gordon, L. A., and Loeb, M. P. (2006). The economics of information security investment. ACM Transactions on Information and System Security (TISSEC), 9(4), pp 438-457.

Gordon, L. A., Loeb, M. P., Lucyshyn, W., and Zhou, L. (2017). A framework for using social science to improve cyber security. *Journal of Cybersecurity*, 3(1), pp 59-69.

Herath, T., and Rao, H. R. (2019). Social science in information security research: An interdisciplinary approach. *Information & Management*, 56(2), pp 225-235.

Jøsang, A. (2017). Teaching cybersecurity through gaming simulations. *IEEE Security & Privacy*, 15(3), pp 89-93.

Kim, Y., and Kim, H. (2019). Teaching cybersecurity ethics through case studies. *Journal of Computing Sciences in Colleges*, 34(2), pp 77-84.

Kshetri, N. (2017). Blockchain's roles in meeting key supply chain management objectives. International Journal of Information Management, 37(2), pp 1-7.

Kumar, S., and Pang, H. (2015). Exploring the human factors of information security incidents. *Computers & Security*, pp 50, 70-80.

Kumaraguru, P., Sheng, S., Acquisti, A., Cranor, L. F., and Hong, J. (2013). Lessons learned from the world of unusable security interfaces. *IEEE Security & Privacy*, 11(1), pp 63-69.

Maguire, M., Donovan, E., and Chen, Y. (2020). Integrating social science topics into a cybersecurity curriculum. *Journal of Information Technology Education: Innovations in Practice*, 19, pp 273-287.

Mangalaraj, G., Nadarajan, R., and Dhuraisamy, R. (2016). A systematic review of organisational context factors influencing information security policy compliance. *Journal of Information Security and Applications*, 29, pp 50-72.

Martin, N. A. (2017). An exploration of virtual reality for teaching information security awareness. *Journal of Information Technology Education: Research*, 16, pp 207-227.

Meyer, E., and Canright, G. S. (2016). The flipped classroom model and problem-based learning: Improving patient safety through enhanced teamwork skills. *Journal of Professional Nursing*, 32(3), pp 191-197.

Mitropoulos, S., Dhillon, G., and Arachchilage, N. A. G. (2018). Human aspects of information security in organisations. *Journal of Business Research*, pp 82, 23-30.

Moor, J. H. (2010). Why we need better ethics for emerging technologies. *Ethics and Information Technology*, 12(1), pp 1-4.

Morrow, R., and Brown, J. (2015). Developing socially responsible information security professionals: Service-learning projects in the information systems security classroom. *Journal of Information Systems Education*, 26(3), pp 181-190.

O'Connor, L. T., and Lada, A. (2018). Active learning in cybersecurity education: A review. *Journal of Information Systems Education*, 29(4), pp 259-269.

Olson, J., and Yousuf, S. (2019). Active learning strategies for integrating social science into cybersecurity education. *Journal of Cybersecurity Education, Research and Practice*, 1(1), pp 19-32.

Singer, J. B., and Friedman, B. (2017). Motivations for hacking. *The Palgrave Handbook of Security, Risk and Intelligence* (pp 103-121). Palgrave Macmillan, London.

Singh, A. K., Bali, R. K., and Sharma, S. K. (2018). Human factors in information security: Review and future directions. *Journal of Organizational and End User Computing (JOEUC)*, 30(4), pp 1-20.

Siponen, M. T., Vance, A., and Willison, R. (2018). Educating employees about information security: Lessons from a survey of companies in Finland. Journal of Information Systems Education, 29(2), 85-96.

UM FCJS; (n.d.). *Undergraduate Study Programme in Information Security*. [online], Faculty of Criminal Justice and Security, University of Maribor, https://fvv.um.si/en/study/undergraduate-study-programmes/information-security/

Van den Berghe, L., and Walgrave, S. (2016). Public support for security policy: A review of the social psychological literature. *Journal of Police and Criminal Psychology*, 31(1), pp 15-28.

Van Niekerk, J. F., and Von Solms, R. (2017). A framework for security awareness training based on attitudes and motivation. *Computers & Security*, 70, pp 1-11.

Whitman, M. E., and Mattord, H. J. (2016). *Principles of information security*. Cengage Learning.