Citizens' Cybersecurity Behavior

Some Major Challenges

Ying Li | Dalian University of Technology
Tong Xin | University of Jyväskylä
Mikko Siponen | University of Jyväskylä

Citizens' cybersecurity behaviors are an important concern in the modern age. This work discusses the challenges of studying citizen cybersecurity behaviors and the directions for future research.

The number of home users has increased rapidly and extended from desktop computers and laptops to tablets, smartphones, and devices connected to the Internet of Things. The age groups of users have also increased from adults to include kids and seniors. At the same time, all these devices, when connected to the Internet, are also potential targets for hackers and virus distributors. Users may realize these threats by ransomware, information theft, malicious ads, and phishing (Figure 1). Significantly, due to the COVID-19 pandemic, many people work from home, which can exacerbate existing risks. Ponemon Institute's recent survey shows that 71% of organizations are very concerned that remote workers are putting them at risk for data breaches/security exploits.[1] In addition to cybersecurity risks, privacy risks are also citizens' concerns, since their private information is often collected and used.

How to strengthen the cybersecurity behavior of citizens is a problem worthy of attention in theory and practice. Despite the importance of citizen cybersecurity and some work in this domain, academic responses to cybersecurity have been generally studied in the organizational context. Furthermore, addressing the cybersecurity behavior of the general population requires new thinking at the government level.

This study conducted a semisystematic review of the literature on behavioral cybersecurity to capture the latest security threats to people and the status of behavioral cybersecurity research over the past five years. Based on the literature review, we summarize some key cybersecurity threats to individuals and raise major challenges in research. This research review leads us to outline future research directions on cybersecurity research and the practices of individual users.

Emerging Cybersecurity Threats in Remote Work

The COVID-19 pandemic has changed the way of life and work around the world. Many people have moved home to work and study. The massive shift has raised significant

Digital Object Identifier 10.1109/MSEC.2021.3117371
Date of current version: 28 October 2021

cybersecurity concerns, as individuals and organizations face new cybersecurity contexts. A global survey for 2020 found that nearly half of the respondents had never worked from home previously and 73% reported not receiving special training on safe interaction with corporate resources over the Internet.[2] Remote work creates several cybersecurity concerns in three aspects.

Unsecured Home Computing Environment

It is unlikely that all companies provide their employees with secure work devices that employees can use at home. Instead, many employees use their personal endpoint devices (e.g., laptops, tablets, mobile phones, among others) to work and connect to the office IT infrastructure from home networks. Most people do not know how to configure a sufficiently secure home network, which can become an unsecure Internet channel and is easily attacked.[3] In addition, remote workers use their personal devices for entertainment, online games, watching movies, and downloading all kinds of software, increasing the possibility of suffering from viruses and malware.

Vulnerabilities in Collaboration Tools

Remote work increases the demand for collaboration tools, such as file sharing, online meetings, and cloud applications. Files sent from the company office to a remote device can become exposed in the process and vice versa. Online meetings can expose data on meeting platforms, such as audio, video, and work files, which can lead to data leakage. Cloud solutions are also challenged to prevent data breaches.

Risky Behavior of Family Members

Remote workers may have additional responsibility to manage the behavior of family members if they share computer devices at home. Children and spouses can have access to an employee's computer to upload and download files and click suspicious links. In addition, people at home are easily distracted, making them prone to relax the security requirements for themselves and family members, from failing to install software security updates in time to having weak passwords and giving up sensitive information to phishing emails.

Cybersecurity Threats Target a Wider Range of People

Cyberattacks that exploit human vulnerabilities are constantly evolving, targeting all people, from seniors to adolescents. Although organizations invest many resources to improve employee security awareness and skills, there are still many people, such as seniors and teens, who are vulnerable to cybersecurity threats. Cybersecurity risks are no longer confined to employees at work, but to anyone who uses the Internet for communication, entertainment, transactions, and social networks. In recent years, the number of children and seniors using computers, smartphones, and the Internet is increasing.

Figure 1. Cybersecurity threats to citizens.

Seniors are one of the most vulnerable groups of Internet users prone to cyberattacks. Seniors usually become the target of Internet scammers, as they may be more susceptible to trusting strangers and often lack confidence in using the Internet. Many scams aim to defraud seniors by obtaining their personal information and pressuring them into paying. These scams are usually initiated by email, social networks, or manipulating browsers. Research shows that seniors are more likely to suffer from malware attacks.[4]

Malware attacks and cybercrime do not live only in the adult world. They also target children and adolescents. Children today spend a substantial amount of time online for educational or entertainment purposes. Children face more cybersecurity risks than ever, such as online privacy risks, social engineering attacks, cyberbullying, and so on. A survey conducted in the United States, China, Brazil, and Italy stated that 75% of children would share personal information online in exchange for goods and services.[5] Children's cybersecurity received a lot of attention in both research and practice to work out ways to ensure children's cybersecurity.[6]

Main Approaches to Improve Cybersecurity Behavior in Research

In the literature on behavioral information security, although the cybersecurity behavior of users was recognized years ago, much research has been conducted in an organizational context, focusing on employee security-related behavior, such as computer abuse, misuse of information systems, and violation of information security policies.[7] Deterrence theory is one of the most commonly applied in this stream of research, suggesting that the certainty and severity of sanctions can deter employees' cybersecurity policy violation behavior. Another widely used theory is the protection motivation theory.[8]

This research stream presents a threat message aimed at "scaring" people to engage in protective cybersecurity behavior. Security education training and awareness (SETA) programs help organizations mitigate security breaches caused by human error. This is accomplished by making people aware of information security policies and being able to apply them during their daily activities to help prevent security incidents.[3] The SETA program helps manage employee behavior on the job.

Challenges in Understanding Citizens' Cybersecurity Behavior

Having taken stock of behavioral cybersecurity research, which is conducted in an organizational context, we are in a position to discuss some of the unstudied challenges for individual cybersecurity behavior. To understand and highlight some of the challenges, we present a framework that highlights some potential differences in cybersecurity behavior between organizational and individual users using the semisystematic literature review approach. The development process of this framework can be summarized into four stages. First, in the review design phase, we clarified the research question (i.e., what are the differences between the information security threats faced by individuals home users and individuals as organizational users), review method, and the search strategy. The second is the conducting phase. We searched databases such as EBSCO, IEEE *Xplore*, JSTOR, Science Direct, Google Scholar, and other websites with keywords: cybersecurity, behavioral cybersecurity, insider threats, organizational user information security, home user information security, and so on. Two reviewers were invited to screen the articles to ensure the quality and reliability of the protocol. Finally, the review sample was determined. The third phase was to analyze the sample. The abstracted data are in the form of descriptive information, and we focused mainly on analyzing the factors that affect the security behavior of the users or individuals in the samples. After discussion by a group consisting of three information systems experts, we suggest that factors affecting user information security behavior can be classified into three aspects: user differences, environment differences, and differences in the interaction between users and the environment. Finally, based on the information in the third phase, we summarize some key differences between organizational and home contexts (see Table 1) and write a review based on the framework, as shown in Figure 2.

Table 1. Some key differences between the organizational context and the home context.

	Differences	Organizational Context	Home Context
User	Demographics	Working population	More differentiated populations such as teens, older adults, housewives/househusbands, family members, friends, and even strangers
	Knowledge	Working people have more organization-based security knowledge	Home users may have limited home-based security knowledge; some of them did not have opportunities to receive security education
	Perception/assessment capability	Relatively high for working people due to thee organization's education and support	Relatively low since some home users are lacking security knowledge and support
Environment	Activities	Mainly work-related	Online shopping, online banking, online communications, entertainment, online education, and so on
	Connected	Less connected devices	More connected devices
	Shared	Low level	High level
	Safety climate	Shaped by organizational members	Shaped by family members
	IT support	Professional	Unprofessional
	Network security	More secure	Less secure
	Policies	Relatively complete	Incomplete
	Awareness training	Formal	Informal
Interaction between users and the environment	Responsibility	Clear	Unclear
	Transparency of responsibility	Visible boundary	Invisible boundary

User Differences

Demographics. Differences in gender, age, education, knowledge, and skills require a different understanding of user security behavior. For example, in organizational user research, the investigated employees are usually middle-aged people with better education backgrounds, and so on. However, due to various home living arrangements, such as the traditional home of family members who live together, friends who live together, or shared apartments where individuals live with strangers, users include a wider range of people. They can be teenagers, older adults, housewives/househusbands, family members, friends, and even strangers who work or do not work in organizations. Demographic differences can lead to different patterns of behavior and require particular explanations. For example, research has found statistically significant gender differences in terms of computer skills, previous experience, signals-to-action, security self-efficacy, and self-reported cybersecurity behavior.[9]

Knowledge. Basic cybersecurity knowledge should include knowledge of computers, networks, and other infrastructure/devices, knowledge of cybersecurity threats and consequences, and knowledge of the corresponding measures and actions. Users in the organizational environment can obtain cybersecurity knowledge through training, professional IT support, and other channels. On the contrary, the vast majority of people often do not adequately understand the operating principles of home networks and devices, as well as security and privacy threats. As a result, there is a gap between people's general awareness of cybersecurity threats and their actual understanding of how threats work. In addition, security attacks targeted at home may be different from those targeting organizations. As a result, users may or may not understand how these threats work, making it more difficult for individuals to take effective security actions. Even some users do not have the desire or time to learn the knowledge; therefore, they cannot handle the risks.

Perception/assessment capacity. Compared to organizational employees, individuals have limited ability to perceive cybersecurity threats and evaluate reliable/available security sources. On the one hand, due to the lack of the necessary knowledge, individual users may not be able to perceive and identify cybersecurity threats at home sensitively. On the other hand, unlike organizational users with multiple forms of support, individual users need to choose security sources or support independently. However, when users need help dealing with cybersecurity threats, their assessment metrics of the quality or ability of the security source are uneven.[10]

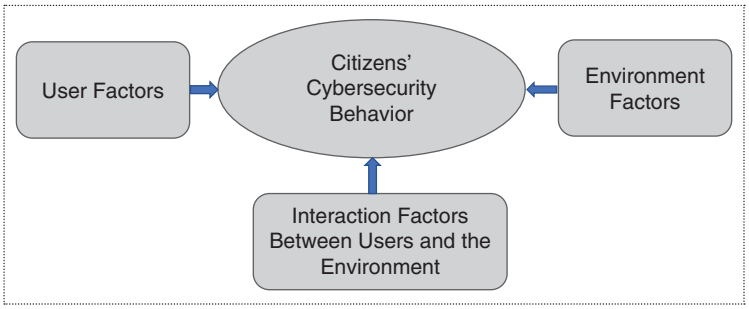

Figure 2. A framework for understanding citizens' cybersecurity behavior.

Environmental Differences

The environment in this study refers to the environment in which users use networks, computers, and other smart devices. It includes all elements related to the cybersecurity of users in the environment, such as devices, technology, services, and social influences. We categorized the elements into two aspects: the characteristics of the environment and the elements that help support cybersecurity (see Figure 3). We also compared the differences between the home environment and the work environment from these two aspects.

Environment. Differences in characteristics between the home and the organizational environment manifest themselves primarily in the multiple activities involved in the environment (activities in the environment), different networked devices in the environment

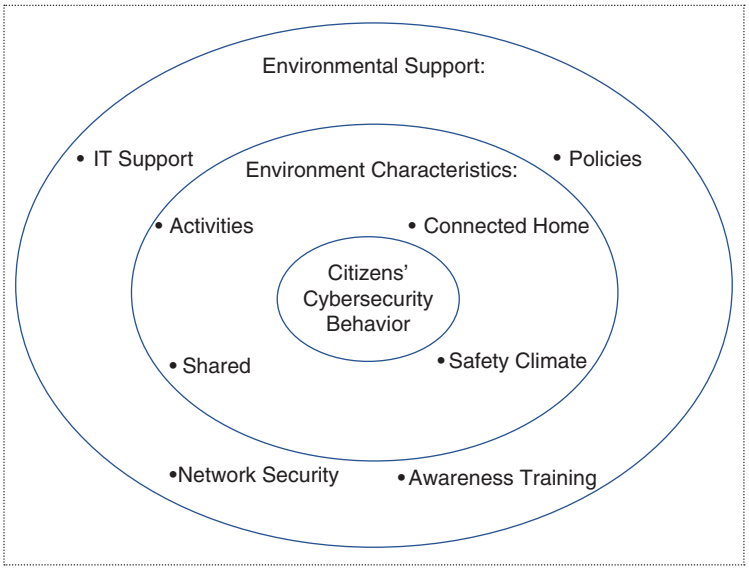

Figure 3. The environmental influences on citizens' cybersecurity behavior.

(connected home environment), the different ways of using the network and devices (shared environment), and the difference in the overall security atmosphere (safety climate).

Activities in the environment. The computer and network-centric activities of the employees in the organization are mainly related to work, which is relatively simple. In comparison, people can carry out various computer and Internet activities at home, such as online shopping, managing savings through online banking, communications, entertainment, online education, and so on. Due to COVID-19 and for other reasons, such as operating costs, some people are required to work from home. Remote work has advantages; however, it also presents risks to the security of personal and company data. Many attacks target teleworkers. For example, online meetings can expose more forms of data on meeting platforms, such as audio, video, and work files, increasing the ways of privacy breach. The diversity of activities can generate more cybersecurity threats, making the home environment more demanding for cybersecurity technology and user awareness of cybersecurity.

Connected home environment. Individual users may underestimate the security risks of the highly connected home environment. Users may have more than 10 devices connected at home, such as computers, mobile phones, cameras, wearables, and sensors. The connected home environment is continuously expanding. Furthermore, the rapid development of smart homes, with unmatched cybersecurity technologies and chaotic management platforms, has made smart home security and privacy another cybersecurity risk at home. Unlike employees in organizations who only need to take care of their work computer-related behaviors, individual home users face increasingly complex security situations.

Shared environment. One characteristic of the home environment is that family members share the home Internet connection and devices. It has become quite typical during the pandemic with people working and studying at home. However, sharing home devices can become a source of tension that disrupts harmonious relations between family members; on the other hand, it can blur the privacy boundaries of family members and even reveal their privacy. This character increases the difficulty in managing cybersecurity at home.

Environmental safety climate. Research suggested that employees who perceived a strong safety climate in the organization worked more safely themselves.[11] The perception was derived from the observation of organizational management, superiors, and peer attitudes. Goo et al. conducted an empirical study and the results showed that the cybersecurity climate encouraged employee compliance behavior.[11] Compared to the norm, a safe climate is very difficult to form at home. It relies on the awareness, desires, and security requirements of each family member. Therefore, a security climate can only be formed with the efforts of all family members.

Support. Cybersecurity supports in the organizational environment can be divided into hard support for devices and networks, such as technical IT support, network security support, and soft support for users, such as policies, awareness training, mandatory control, and monitoring. However, such hard supports are almost absent in the home environment and generally come from third-party cybersecurity services paid by users or informal support from social relationships.[10] Soft supports in the home environment (such as subjective norms) come more from the impact of family members, peers, mass media, and so on, on users in cybersecurity. Most of these supports rely on users to actively search for and evaluate their qualities. We discuss this in detail in the following.

IT support. Organizations can implement a security plan. They can invest large amounts of money, time, and resources. It makes it easy for employees to get security support on software and hardware and timely human assistance. However, for the end user in the home context, investment in security is limited or nonexistent.[12] Insurance for security and continuous security service is still missing for many individuals and families. Organizations are not supposed to help users solve their problems while browsing entertainment video websites or to warn people to use a strong Facebook password. Instead, people usually obtain relevant guidelines online, which requires extra effort. Alternatively, people may seek the help of friends or a paid service. However, such resources are often unprofessional or costly. Therefore, when people perform nonwork-related computing, they may perceive limited facilitating conditions, which may be less helpful in solving security problems compared to those in a work situation. Research found that the facilitation conditions were not related to the use of strong personal passwords, indicating that the facilitation conditions have a stronger impact on work-related security behavior than nonwork-related security behavior.[13]

Network security. Network security, on the one hand, depends on the protection of hardware and software.

Due to the IT support organizations offer, such as firewalls and antimalware software, organizations are well prepared for Internet attacks. However, people may invest less in hardware and software in the home context, resulting in a low level of network security. On the other hand, network security is based on the maintenance of the system by the user. In an organization, there are IT specialists to explore potential network risks and solve problems. In the home context, unless the user has related knowledge and problem-solving ability, most users who do not take measures to protect networks face the possibility of being attacked by intruders.

Policies. Cybersecurity policy is an important component of a management system in an organization. Usually, the policy contains regulations on the following aspects: network, devices, data, operation, sanctions, and so on.[14] The policy is a guideline for security management and a code of conduct for employees. It instructs employees how to use information resources correctly and safely, while it deters employees from violating the policy. A cybersecurity policy greatly contributes to keeping information safe. Therefore, policy is an important feature in the organizational context. However, most cybersecurity policies are not limited to the workplace. If employees work outside the office, they also have the responsibility to ensure the safety of organizational materials. Unfortunately, most organizations lack explicit security policies that employees can follow when they work from home. Some of the policies take effect no matter where employees are working. Therefore, IT managers must revisit current policies to ensure both security and applicability in remote work environments. The policies to be updated may include the recommended practices at home, such as using company-approved devices to handle work-related tasks, forbidding sharing device passwords with family members, and so on. Privacy policies must be updated to consider new ways for employees to access information, such as online meetings.

Awareness training. Firms often design educational and training programs for cybersecurity. However, in the home context, by and large, end users hardly receive formal cybersecurity awareness training. Their knowledge of cybersecurity comes mainly from self-learning and self-experience. Of course, some people may have received training at their workplace, but there is no empirical evidence indicating whether it transfers to increased home security. Applicable awareness training programs should be developed to help citizens deal with security threats, such as what constitutes a security threat, how to recognize a security threat, and what actions to take to deal with threats.

Differences in the Interaction Between Users and the Environment

The user is in the environment, and it is inevitable that you interact with the elements in the environment. The interactions between users and the environment regarding cybersecurity occur mainly with network/devices and with other people/organizations in the environment.

Responsibility. Complying with the cybersecurity policy and taking care of one's own computer seems to be the responsibility of employees in the organizational environment. The responsibility of protecting information and privacy security that individual users need to bear is more complicated. It includes the perceived personal responsibility of users and the scope of responsibility they believe to be undertaken, such as protecting their computers. It also includes invisible responsibility in the home environment, that is, users' responsibility for shared devices or networks in the home, such as routers, networks, or smart home devices. Some users are even responsible for the cybersecurity of other people at home. For example, capable children make cybersecurity decisions on behalf of parents who lack cybersecurity knowledge. Due to the different scope of responsibility, family members may play different roles at home to ensure security. In addition, research has identified tensions that arise due to different responsibilities of family members. It could be a dangerous situation if the administrator of the home IT system uses the technology to spy on or deny access to other family members.[15]

Transparency of responsibility. What follows with responsibility is the transparency of responsibility, that is, the degree to which people understand the boundaries of their responsibilities. The boundaries of invisible responsibilities in the home environment are often blurred. For example, individual users may not think they are responsible for the information and privacy of vulnerable family members. Alternatively, in contrast, they are too eager to help others and go beyond the boundaries of family users. The power of users who actively and passively participate in cybersecurity behaviors is not equal. Furthermore, even the perceived responsibility of people has blurred boundaries, and it may not be just the problem of users. For example, the security and privacy concerns of the smart home Internet of Things are mainly due to the unclear scope of the respective responsibilities of different parties. The responsibilities could be on the software development side, vendors side, cybersecurity service side, or user side. They may believe that some cybersecurity operations were the responsibility of the other party and did not take any cybersecurity action, resulting in a vulnerable area in the cybersecurity environment of the home. In contrast, due

to the clear cybersecurity policy, effective training, and guidance of the organization, employees have a relatively high degree of transparency in responsibility. Responsibility and transparency of responsibility have never been mentioned in previous studies of individual users, but they affect cybersecurity behaviors.

Cybersecurity has become an important issue, a topic of relevance to virtually all people. Despite that, the primary focus of behavioral cybersecurity research has been on an organizational context. While such research in an organizational context is important, theory and research on user cybersecurity also require serious attention from scholars. Although there are similarities between the cybersecurity behavior of home users and the cybersecurity behavior of employees in an organizational context, it is necessary to understand their differences and allow research and practice on the cybersecurity behavior of individuals to develop further. As a first step in improving the situation, we discussed some differences between these contexts. These include user differences, environmental differences, and differences in the interaction between users and the environment. Finally, an even more fundamental issue is sociopolitical: improving citizen cybersecurity behavior requires some educational interventions. In the organizational context, the organization can give these. But in the case of individual home users' cybersecurity behavior, who is making these interventions? The best option, in terms of being more systematic and universal, would be government-led activities. Understanding this would require a new set of organizational structures and activities at the government level. Governments can conduct cybersecurity awareness campaigns to change risky behavior of citizens. Campaigns should differ when targeting different groups of citizens, in different risky situations, and at home or in other public contexts. Research and thinking on these matters are lacking. ■

Acknowledgments

This study was funded by the National Social Science Fund of China (18CGL045). We thank the editor and the reviewers for their comments and suggestions.

References

1. "Cybersecurity in the remote work era: A global risk report," Ponemon Inst., Traverse City, MI, Oct. 2020. [Online]. Available: https://www.keeper.io/hubfs/PDF/Cybersecurity%20in%20the%20Remote%20Work%20Era%20-%20A%20Global%20Risk%20Report.pdf
2. "How COVID-19 changed the way people work," Kaspersky. Accessed: Sept. 25, 2021. [Online]. Available: https://media.kasperskydaily.com/wp-content/uploads/sites/92/2020/05/03191550/6471_COVID-19_WFH_Report_WEB.pdf
3. M. Karjalainen, M. Siponen, and S. Sarker, "Towards a theory of information systems security behaviors of organizational employees: A dialectical perspective," *Inf. Syst. Res.*, vol. 30, no. 2, pp. 687–704, 2019. doi: 10.1287/isre.2018.0827.
4. R. Shinde, P. Van der Veeken, S. Van Schooten, and J. van den Berg," Ransomware: Studying transfer and mitigation," in *Proc. Int. Conf. Comput. Anal. Security Trends*, 2016, pp. 90–95. doi: 10.1109/CAST.2016.7914946.
5. "Kids online safety–Internet safety for kids," Safeatlast, Dec. 2020. [Online]. Available: https://safeatlast.co/blog/kids-online-safety/#gref
6. F. Quayyum, D. S. Cruzes, and L. Jaccheri, "Cybersecurity awareness for children: A systematic literature review," *Int. J. Child-Comput. Interact.*, vol. 30, p. 100,343, Dec. 2021. doi: 10.1016/j.ijcci.2021.100343.
7. G. Moody, M. Siponen, and S. Pahnila, "Toward a unified model of information security policy compliance," *MIS Quart.*, vol. 42, no. 1, pp. 285–311, 2018. doi: 10.25300/MISQ/2018/13853.
8. S. Haag, M. Siponen, and F. Liu, "Protection motivation theory in information systems security research: A review of the past and a road map for the future," *ACM SIGMIS Data Base Adv. Inf. Syst.*, vol. 52, no. 2, pp. 25–67, 2021. doi: 10.1145/3462766.3462770.
9. M. Anwar, W. He, I. Ash, X. Yuan, L. Li, and L. Xu, "Gender difference and employees' cybersecurity behaviors," *Comput. Hum. Behav.*, vol. 69, pp. 437–443, Dec. 2016. doi: 10.1016/j.chb.2016.12.040.
10. N. Nthala and I. Flechais, "Informal support networks: An investigation into home data security practices," in *Proc. 14th Symp. Usable Privacy Security (SOUPS)*, 2018, pp. 63–82. [Online]. Available: https://www.usenix.org/conference/soups2018/presentation/nthala
11. J. Goo, M. S. Yim, and D. J. Kim, "A path to successful management of employee security compliance: An empirical study of information security climate," *IEEE Trans. Prof. Commun.*, vol. 57, no. 4, pp. 286–308, 2014. doi: 10.1109/tpc.2014.2374011.
12. M. Dupuis, T. Geiger, M. Slayton, and F. Dewing, "The use and non-use of cybersecurity tools among consumers: Do they want help?" in *Proc. 20th Ann. SIG Conf. Inf. Technol. Educ.*, 2019, pp. 81–86. doi: 10.1145/3349266.3351419.
13. Y. Li, T. Pan, and N. Zhang, "Examining the boundary effect of information systems security behavior under different usage purposes," *IEEE Access*, vol. 7, pp. 156,544–156,554, Oct. 2019. doi: 10.1109/access.2019.2949079.
14. H. Kinnunen, M. Siponen, and M. Lapke, "State of the art in information security policy development," *Comput. Secur.*, vol. 88, p. 101,608, Sept. 2019. doi: 10.1016/j.cose.2019.101608.
15. E. Zeng, S. Mare, and F. Roesner, "End user security and privacy concerns with smart homes," in *Proc. 13th Symp.*

Usable Privacy Security (SOUPS), 2017, pp. 65–80. [Online]. Available: https://www.usenix.org/conference/soups2017/technical-sessions/presentation/zeng

Ying Li is an associate professor in the School of Economics and Management, Dalian University of Technology, Dalian, Liaoning, 116024, China. Her research interests include users' security and privacy behavior, data security in open government, and user behavior in social commerce. Li received a Ph.D. in information processing science from the University of Oulu, Finland. Contact her at yingli@dlut.edu.cn.

Tong Xin is a Ph.D. candidate in the Faculty of Information Technology at the University of Jyväskylä Jyväskylä, 40100, Finland. Her research interests include social cognitive psychology and information security behaviors. Xin received a master's degree in psychology from Anhui Normal University, China. Contact her at toxin@student.jyu.fi.

Mikko Siponen is a professor of information systems at the University of Jyväskylä Jyväskylä, 40100, Finland. His research interests include information security, philosophy of science, cyber crimes, and IT ethics. Siponen received a Ph.D. in applied philosophy from the University of Joensuu, Finland, an M.Sc. in software engineering, and a Ph.D. in information systems from the University of Oulu, Finland. He has received several million euros in research funding from corporations and many other funding bodies. He is an invited member of The Finnish Academy of Science and Letters. Contact him at mikko.t.siponen@jyu.fi.