How a Security Adoption Process Model Might Differ for Information Workers

Cori Faklaris, *Department of Software and Information Systems,*
College of Computing and Informatics, University of North Carolina at Charlotte, NC, USA

Abstract

Given the behavioral complexities of cybersecurity, information security workers would benefit from a model of security practice adoption that is tailored to the organizational context. In this workshop paper, I describe my research to date to synthesize a preliminary model for U.S. internet users aged 18 or above. I then pose a series of open questions as to how this preliminary model may need to be modified for the security information work context. The discussion will inform follow-up work to examine the process of security information behavior adoption at the level of system users' policy compliance and workarounds, at the level of senior administrators' configuration of security affordances for critical infrastructure, and at the level of information workers' interaction with others in the social role of a tech helper.

1. Motivation

Computing systems are increasingly central to society, but many people do not understand enough about how they work or what cyber-threats to guard against [16], contributing to a global cybercrime cost of over $1 trillion [39]. While many good solutions exist (such as using password managers), people have been slow to become fully aware of what they do and to use them regularly [24,41,46]. Further, enterprise training can cost $300,000 and hundreds of staff hours [37].

To reduce costs and improve awareness and adoption, we should look to insights from social psychology, marketing, and public health, e.g. work on Funnels [5], Learning-Adoption Trajectories [34,35], Stages and Processes of Change [25,26], and Innovation Diffusion [17,32]. These show that behavior change unfolds as a process in time and can be influenced by contacts that are relevant at a given stage of the process; also, that interventions are more successful when guided by appropriate theory [6,10,13,19]. A common thread is that the target audience for behavior change is analyzed and split into segments, either by stage in the change process or by individual characteristics. Researchers then can zoom in and identify the processes or factors that differentiate each segment and that can explain the evolution in time of thinking and emotions about the target behavior. This avoids a "one size fits all" approach and produces a classification scheme that can be used to design and direct an intervention to those who are most likely to benefit from it.

No one has yet established or validated such a model for use by security information workers (system administrators, security staff, developers, those who regularly handle personally identifiable information or other sensitive data, etc.). Cybersecurity needs this new model. It is a more complex behavior system than those modeled in prior work, involving social interactions that occur both online and offline (for which time and place, anonymity, physical appearance, and physical distance can be very different [1,2,21]). Moreso than elsewhere in human-computer interaction, cybersecurity involves multiple actors with conflicting objectives (attackers, both internal and external, vs. an array of legitimate non-malicious users, such as administrators and end users), for whom usage of the same technologies will vary dramatically [3]. It also is unlike physical security, say for nuclear defense, because it is much messier in terms of number and kinds of actors, involving massively more distributed technologies, the lack of a shared consensual outcome among all stakeholders, and disagreements about acceptable tradeoffs [36,44].

2. Research to Date

Prior has shown that, as with mask-wearing [15] or vaccinations [14], people's attitudes [11] and social contexts [22,40] factor into the extent to which they engage in protective behaviors for cybersecurity, such as checking that their antivirus software is up-to-date or keeping their network password confidential. Fear appeals are important [4,20,33] but not sufficient to persuade people to adopt cybersecurity practices [45]; they also need awareness, motivation, and knowledge of how to use these practices to protect against threats, a framework known as security sensitivity [8,20,33]. Security sensitivity, in turn, has been shown to be informed by social influences, such as whether a trusted family member or authority figure gives advice about which security practices to use [30,31], whether people hear stories that teach them about security practices [27–29,43], or whether people observe trusted contacts such as friends engaging in secure behaviors [7–9]. These influences may lead to long-term adoption, or to rejection if peers/media share negative experiences [12,46].

I have used an exploratory sequential mixed-methods approach to specify a preliminary model of the security adoption process for end users, comprised of six steps of adoption,

USENIX Symposium on Usable Privacy and Security (SOUPS) 2022. August 7-9, 2019, Boston, MA, USA, and virtual.

their step-associated social influences, and each step's obstacles to moving forward. I first conducted a nationally recruited, remote interview study with U.S. internet users age 18 and older (*N*=17) to synthesize a common narrative of how people adopt security practices. I next designed and deployed an online survey study (*N*=859) to validate the interview insights with a U.S. Census-matched panel of internet users aged 18 and older. I then integrated these findings and triangulated them with prior research on the influences of threat awareness, social proof, advice-seeking, and caretaking roles in people's security behaviors (Figure 1).

To classify participants into the model's steps of adoption, I created and tested the following survey algorithm, which successfully sorted each participant into one and only one step of security practice adoption:

1. Are you currently using [the security practice]? *Binary response set: Yes/No*
2. [If Yes] When did you start using [the security practice]? *Binary response set: Up to 6 months ago/6 months ago or longer*
    a. [If <6] STEP 3: IMPLEMENTATION
    b. [If >=6] STEP 4: MAINTENANCE
3. [If No] Did you ever use [the security practice]? *Binary response set: Yes/No*
    a. [If Yes] STEP X: REJECTION(a)
4. [If No] What best fits your situation regarding [the security practice]? *Multiple-choice response set: I am aware of it but decided not to use it/I am aware of it and willing to start using it, but haven't yet/I am aware of it but hesitant to start using it/I am not aware of [the security practice]/I forgot about [the security practice]*
    a. [If Decision] STEP X: REJECTION(b)
    b. [If No Decision, but Aware] STEP 2: SECURITY LEARNING
5. [If Not Aware or Forgot] Do you know of any threats to your online data or accounts that use of [the security practice] will guard against? *Binary response set: Yes/No*
    a. [If Yes] STEP 1: THREAT AWARENESS
    b. [If No] STEP 0: NO LEARNING OR THREAT AWARENESS

Participants in remote interviews were first surveyed about their awareness and adoption of 13 security practices and questioned further about their use of 2-3 of these practices. These included creating strong passwords, creating unique passwords, using multi-factor authentication, using a built-in password manager or a separately installed password manager, using antivirus software, staying alert for and reporting phishing emails, checking for https in URLs, using internet search to verify the legitimacy of online posts, and physically securing their smartphones. Survey respondents were randomly assigned to questions about using a built-in password manager or using a separately installed password manager.

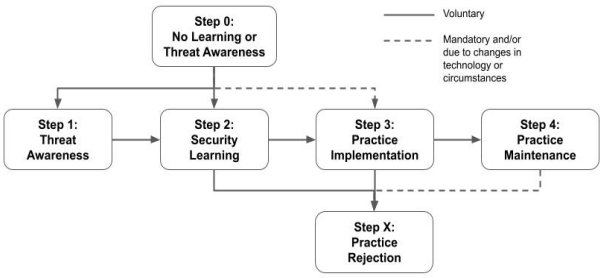

Figure 1: The path model of the steps of security practice adoption that emerged from interviews and survey responses has six steps: Step 0: No Learning or Threat Awareness, Step 1: Threat Awareness, Step 2: Security Learning, Step 3: Practice Implementation, Step 4: Practice Maintenance, and Step X: Practice Rejection. Some paths are marked with a dotted line if they are mandatory, solid paths are voluntary. Survey participants were classified into the steps using the algorithm described in the text.

3. Open Questions for Discussion

The above model was developed with ordinary end users in the context of consumer-grade usable security. It may be that a separate model will need to be developed and validated for use in security-information work inside organizations. To that end, the following questions are open for discussion.

3.1. Which Stakeholders Should Be Represented, If Any?

Security policy for information is usually set a few levels above the system user or the junior security information worker: by system administrators who may not work directly with the frontline IT workers, or by the Chief Security Information Officer (CISO). These policies are often what dictate whether the organization implements security practices that can protect critical infrastructure [23], such as using two-factor authentication for smartphones or requiring that enterprise passwords be regularly checked against lists of known compromised credentials [47]. Organizations such as banks, hospitals, and schools may also employ directors for regulatory compliance management and governance, using frameworks such as Control Objectives for Information Technology (COBIT) [48] or the Unified Compliance Framework (UCF) [49].

Some questions that this suggests: Does this type of policy development and implementation replace or modify the existing path from Step 1: Threat Awareness to Step 2: Security Learning and Step 3: Security Practice Implementation? What kinds of obstacles are likely to exist in this path that contribute to organizations failing to implement needed safeguards for critical infrastructure? Does Step 4: Maintenance

require organizations to exhibit active maintenance, in the form of penetration testing or other verification of their security's integrity, or should that be broken out as an extra step?

3.2. How Mandatory is 'Mandatory'? Is Anything 'Voluntary'?

Following on the stakeholder discussion: organizations will often have in place an information security policy that puts all system users on notice of their consent to monitoring and their requirement to follow the security rules put in place by the authorities. However, researchers know that many system users will not follow these rules to the letter and that informal security arrangements or workarounds will be implemented by workgroups [18,38,40,42].

Some questions that this suggests: Would the steps of security adoption in this context follow a path like the dotted line in Figure 1, with Step 0: No Learning or Threat Awareness leading directly to Step 3: Security Practice Implementation? Or should an intermediate step be added, perhaps titled "Security Practice Negotiation"? Perhaps Step 3 should be modified and bifurcated into "Security Policy Compliance" and "Security Policy Workaround"?

3.3. Where Do Peer Social Influences Make a Difference?

It may be reasonable, in this context of mandatory security and on-high security information policy, to assume that security information workers are more advanced than ordinary system users: perhaps automatically placed in Step 4: Maintenance, while system users outside of these departments may only be classified as Step 3: Implementation. But perhaps information security workers need a different model that accounts for their job role in helping to ensure the confidentiality, integrity, and availability of computational data.

Some questions that this suggests: Can security information workers assume specific social roles like peers or media in diffusing security knowledge, akin to how ordinary users look to security opinion leaders or informal tech helpers for guidance? How do they influence each other and their bosses in the bureaucracy? How can a model of the steps of the process integrate with best practices for making these roles explicit, such as designating superusers among rank-and-file workers or IT "cybersecurity buddies" [42,50]?

4. Conclusion

Given the behavioral complexities of cybersecurity, information security workers would benefit from a model of security practice adoption that is tailored to the organizational context. In this workshop paper, I described my research to date to synthesize a preliminary model for U.S. internet users age 18 or above. I then posed a series of open questions as to how this preliminary model may need to be modified for the security information work context. The discussion will inform follow-up work to examine the process of security information behavior adoption at the level of system users' policy compliance and workarounds, at the level of senior administrators' configuration of security affordances for critical infrastructure, and at the level of information workers' interaction with others in the social role of a tech helper.

References

[1] John A. Bargh and Katelyn Y. A. McKenna. 2004. The Internet and Social Life. *Annu. Rev. Psychol.* 55, 1 (2004), 573–590. DOI:https://doi.org/10.1146/annurev.psych.55.090902.141922

[2] John A. Bargh, Katelyn Y. A. McKenna, and Grainne M. Fitzsimons. 2002. Can You See the Real Me? Activation and Expression of the "True Self" on the Internet. *J. Soc. Issues* 58, 1 (2002), 33–48. DOI:https://doi.org/10.1111/1540-4560.00247

[3] Denis Besnard and Budi Arief. 2004. Computer security impaired by legitimate users. *Comput. Secur.* 23, 3 (May 2004), 253–264. DOI:https://doi.org/10.1016/j.cose.2003.09.002

[4] Scott Boss, Dennis Galletta, Paul Benjamin Lowry, Gregory D. Moody, and Peter Polak. 2015. *What Do Systems Users Have to Fear? Using Fear Appeals to Engender Threats and Fear that Motivate Protective Security Behaviors*. Social Science Research Network, Rochester, NY. Retrieved July 18, 2018 from https://papers.ssrn.com/abstract=2607190

[5] Anatoli Colicev, Ashish Kumar, and Peter O'Connor. 2019. Modeling the relationship between firm and user generated content and the stages of the marketing funnel. *Int. J. Res. Mark.* 36, 1 (March 2019), 100–116. DOI:https://doi.org/10.1016/j.ijresmar.2018.09.005

[6] Sunny Consolvo, David W. McDonald, and James A. Landay. 2009. Theory-driven Design Strategies for Technologies That Support Behavior Change in Everyday Life. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (CHI '09), ACM, New York, NY, USA, 405–414. DOI:https://doi.org/10.1145/1518701.1518766

[7] Sauvik Das, Laura A. Dabbish, and Jason I. Hong. 2019. A Typology of Perceived Triggers for End-User Security and Privacy Behaviors. In *Proceedings of the Symposium on Usable Privacy and Security (SOUPS)*, USENIX Association Berkeley, CA. Retrieved August 28, 2019 from https://www.usenix.org/conference/soups2019/presentation/das

[8] Sauvik Das, Tiffany Hyun-Jin Kim, Laura A. Dabbish, and Jason I. Hong. 2014. The effect of social influence on security sensitivity. In *Proceedings of the Symposium on Usable Privacy and Security*, USENIX Association Berkeley, CA. Retrieved from https://www.usenix.org/system/files/conference/soups2014/ soups14-paper- das.pdf

[9] Sauvik Das, Adam D.I. Kramer, Laura A. Dabbish, and Jason I. Hong. 2015. The Role of Social Influence in Security Feature Adoption. In *Proceedings of the 18th ACM Conference on Computer Supported*

Cooperative Work & Social Computing (CSCW '15), ACM, New York, NY, USA, 1416–1426. DOI:https://doi.org/10.1145/2675133.2675225

[10] Rachel Davis, Rona Campbell, Zoe Hildon, Lorna Hobbs, and Susan Michie. 2015. Theories of behaviour and behaviour change across the social and behavioural sciences: a scoping review. *Health Psychol. Rev.* 9, 3 (August 2015), 323–344. DOI:https://doi.org/10.1080/17437199.2014.941722

[11] Cori Faklaris, Laura Dabbish, and Jason I Hong. 2019. A Self-Report Measure of End-User Security Attitudes (SA-6). In *Proceedings of the Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*, USENIX Association Berkeley, CA, Santa Clara, CA, 18. Retrieved from https://www.usenix.org/system/files/soups2019-faklaris.pdf

[12] Cori Faklaris, Laura Dabbish, and Jason I. Hong. 2022. Do They Accept or Resist Cybersecurity Measures? Development and Validation of the 13-Item Security Attitude Inventory (SA-13). *ArXiv220403114 Cs* (April 2022). Retrieved April 25, 2022 from http://arxiv.org/abs/2204.03114

[13] Karen Glanz and Donald B. Bishop. 2010. The Role of Behavioral Science Theory in Development and Implementation of Public Health Interventions. *Annu. Rev. Public Health* 31, 1 (2010), 399–418. DOI:https://doi.org/10.1146/annurev.publhealth.012809.103604

[14] Helge G. Hollmeyer, Frederick Hayden, Gregory Poland, and Udo Buchholz. 2009. Influenza vaccination of health care workers in hospitals—A review of studies on attitudes and predictors. *Vaccine* 27, 30 (June 2009), 3935–3944. DOI:https://doi.org/10.1016/j.vaccine.2009.03.056

[15] James R Mahalik, Michael Di Bianca, and Michael P Harris. 2021. Men's attitudes toward mask-wearing during COVID-19: Understanding the complexities of mask-ulinity. *J. Health Psychol.* (February 2021). DOI:https://doi.org/10.1177/1359105321990793

[16] Ruogu Kang, Laura Dabbish, Nathaniel Fruchter, and Sara Kiesler. 2015. "My Data Just Goes Everywhere:" User Mental Models of the Internet and Implications for Privacy and Security. In *Symposium on Usable Privacy and Security (SOUPS)*, USENIX Association Berkeley, CA, 39–52. Retrieved from https://www.usenix.org/conference/soups2015/proceedings/presentation/kang

[17] J A Kelly, J S St Lawrence, L Y Stevenson, A C Hauth, S C Kalichman, Y E Diaz, T L Brasfield, J J Koob, and M G Morgan. 1992. Community AIDS/HIV risk reduction: the effects of endorsements by popular people in three cities. *Am. J. Public Health* 82, 11 (November 1992), 1483–1489. DOI:https://doi.org/10.2105/AJPH.82.11.1483

[18] Iacovos Kirlappos, Simon Parkin, and M. Angela Sasse. 2015. "Shadow Security" As a Tool for the Learning Organization. *SIGCAS Comput Soc* 45, 1 (February 2015), 29–37. DOI:https://doi.org/10.1145/2738210.2738216

[19] Predrag Klasnja, Sunny Consolvo, and Wanda Pratt. 2011. How to Evaluate Technologies for Health Behavior Change in HCI Research. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (CHI '11), ACM, New York, NY, USA, 3063–3072. DOI:https://doi.org/10.1145/1978942.1979396

[20] James E Maddux and Ronald W Rogers. 1983. Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *J. Exp. Soc. Psychol.* 19, 5 (September 1983), 469–479. DOI:https://doi.org/10.1016/0022-1031(83)90023-9

[21] Katelyn Y. A. McKenna and John A. Bargh. 1999. Causes and Consequences of Social Interaction on the Internet: A Conceptual Framework. *Media Psychol.* 1, 3 (September 1999), 249–269. DOI:https://doi.org/10.1207/s1532785xmep0103_4

[22] Cheul Young Park, Cori Faklaris, Siyan Zhao, Alex Sciuto, Laura Dabbish, and Jason Hong. 2018. Share and Share Alike? An Exploration of Secure Behaviors in Romantic Relationships. In *Proceedings of the Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*, USENIX Association Berkeley, CA, Baltimore, Md., USA, 83–102. Retrieved February 26, 2019 from https://www.usenix.org/conference/soups2018/presentation/park

[23] Nilay Patel. 2021. Hard lessons of the SolarWinds hack. *The Verge*. Retrieved February 13, 2022 from https://www.theverge.com/2021/1/26/22248631/solarwinds-hack-cybersecurity-us-menn-decoder-podcast

[24] Sarah Pearman, Shikun Aerin Zhang, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. 2019. Why people (don't) use password managers effectively. 319–338. Retrieved July 15, 2021 from https://www.usenix.org/conference/soups2019/presentation/pearman

[25] J. O. Prochaska and W. F. Velicer. 1997. The transtheoretical model of health behavior change. *Am. J. Health Promot. AJHP* 12, 1 (October 1997), 38–48.

[26] James O. Prochaska and Carlo C. DiClemente. 1983. Stages and processes of self-change of smoking: Toward an integrative model of change. *J. Consult. Clin. Psychol.* 51, 3 (1983), 390–395. DOI:https://doi.org/10.1037/0022-006X.51.3.390

[27] Christina A. Rader, Richard P. Larrick, and Jack B. Soll. 2017. Advice as a form of social influence: Informational motives and the consequences for accuracy. *Soc. Personal. Psychol. Compass* 11, 8 (August 2017), n/a-n/a. DOI:https://doi.org/10.1111/spc3.12329

[28] Emilee Rader and Rick Wash. 2015. Identifying patterns in informal sources of security information. *J.*

Cybersecurity 1, 1 (September 2015), 121–144. DOI:https://doi.org/10.1093/cybsec/tyv008

[29] Emilee Rader, Rick Wash, and Brandon Brooks. 2012. Stories as informal lessons about security. In *Proceedings of the 8th Symposium on Usable Privacy and Security (SOUPS '12)*, USENIX Association Berkeley, CA, 1. DOI:https://doi.org/10.1145/2335356.2335364

[30] E. M. Redmiles, A. R. Malone, and M. L. Mazurek. 2016. I Think They're Trying to Tell Me Something: Advice Sources and Selection for Digital Security. In *2016 IEEE Symposium on Security and Privacy (SP)*, 272–288. DOI:https://doi.org/10.1109/SP.2016.24

[31] Elissa M. Redmiles, Sean Kross, and Michelle L. Mazurek. 2016. How I Learned to Be Secure: A Census-Representative Survey of Security Advice Sources and Behavior. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security* (CCS '16), ACM, New York, NY, USA, 666–677. DOI:https://doi.org/10.1145/2976749.2978307

[32] Everett M. Rogers. 2010. *Diffusion of Innovations, 4th Edition*. Simon and Schuster.

[33] Ronald W. Rogers. 1975. A Protection Motivation Theory of Fear Appeals and Attitude Change. *J. Psychol.* 91, 1 (September 1975), 93–114. DOI:https://doi.org/10.1080/00223980.1975.9915803

[34] Ismail Sahin. 2005. UNDERSTANDING FACULTY ADOPTION OF TECHNOLOGY USING THE LEARNING/ADOPTION TRAJECTORY MODEL: A QUALITATIVE CASE STUDY. *Turk. Online J. Educ. Technol.* 4, 1 (2005), 10.

[35] Ismail Sahin and Ann Thompson. 2007. Analysis of Predictive Factors That Influence Faculty Members Technology Adoption Level. *J. Technol. Teach. Educ.* 15, 2 (April 2007), 167–190. Retrieved July 28, 2021 from https://www.learntechlib.org/primary/p/18935/

[36] Bruce Schneier. 2008. The Psychology of Security. In *Progress in Cryptology – AFRICACRYPT 2008* (Lecture Notes in Computer Science), Springer, Berlin, Heidelberg, 50–79. DOI:https://doi.org/10.1007/978-3-540-68164-9_5

[37] Tara Seals. 2017. Cost of User Security Training Tops $290K Per Year. *Infosecurity Magazine*. Retrieved January 20, 2021 from https://www.infosecurity-magazine.com:443/news/cost-of-user-security-training/

[38] Mario Sillic. 2019. Critical impact of organizational and individual inertia in explaining non-compliant security behavior in the Shadow IT context. *Comput. Secur.* 80, (January 2019), 108–119. DOI:https://doi.org/10.1016/j.cose.2018.09.012

[39] Zhanna Malekos Smith, Eugenia Lostri, and James A Lewis. 2020. *The Hidden Costs of Cybercrime*. McAfee.

[40] Yunpeng Song, Cori Faklaris, Zhongmin Cai, Jason I. Hong, and Laura Dabbish. 2019. Normal and Easy: Account Sharing Practices in the Workplace. *Proc ACM Hum-Comput Interact* 3, CSCW (November 2019), 83:1-83:25. DOI:https://doi.org/10.1145/3359185

[41] Peter Story, Daniel Smullen, Yaxing Yao, Alessandro Acquisti, Lorrie Faith Cranor, Norman Sadeh, and Florian Schaub. 2021. Awareness, Adoption, and Misconceptions of Web Privacy Tools. *Proc. Priv. Enhancing Technol.* 2021, 3 (July 2021), 308–333. DOI:https://doi.org/10.2478/popets-2021-0049

[42] Serena Wang, Cori Faklaris, Junchao Lin, Laura Dabbish, and Jason I. Hong. 2022. "It's Problematic but I'm not Concerned": University Perspectives on Account Sharing. *Proc. ACM Hum.-Comput. Interact.* 6, CSCW1 (March 2022), 1–27. DOI:https://doi.org/10.1145/3512915

[43] Rick Wash. 2010. Folk Models of Home Computer Security. In *Proceedings of the Sixth Symposium on Usable Privacy and Security* (SOUPS '10), ACM, New York, NY, USA, 11:1-11:16. DOI:https://doi.org/10.1145/1837110.1837125

[44] Steven Weber. 2017. Coercion in cybersecurity: What public health models reveal. *J. Cybersecurity* 3, 3 (November 2017), 173–183. DOI:https://doi.org/10.1093/cybsec/tyx005

[45] Dirk Weirich and Martina Angela Sasse. 2001. Pretty good persuasion: a first step towards effective password security in the real world. In *Proceedings of the 2001 workshop on New security paradigms* (NSPW '01), Association for Computing Machinery, New York, NY, USA, 137–143. DOI:https://doi.org/10.1145/508171.508195

[46] Yixin Zou, Kevin Roundy, Acar Tamersoy, Saurabh Shintre, Johann Roturier, and Florian Schaub. 2020. Examining the Adoption and Abandonment of Security, Privacy, and Identity Theft Protection Practices. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, ACM, Honolulu HI USA, 1–15. DOI:https://doi.org/10.1145/3313831.3376570

[47] Colonial Pipeline Cyber Attack: Hackers Used Compromised Password - Bloomberg. Retrieved February 13, 2022 from https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password

[48] COBIT | Control Objectives for Information Technologies. *ISACA*. Retrieved June 21, 2022 from https://www.isaca.org/resources/cobit

[49] Regulatory Compliance Software for IT Professionals. *Unified Compliance*. Retrieved June 21, 2022 from https://www.unifiedcompliance.com/

[50] Why you need a security buddy (and how to find one) | CSO Online. Retrieved November 22, 2020 from https://www.csoonline.com/article/2133470/why-you-need-a-security-buddy--and-how-to-find-one-.html