Will SOC Telemetry Data Improve Predictive Models of User Riskiness? A Work in Progress

Michael Curry[1]
School of Electrical Engineering and Computer Science, Oregon State University, Corvallis, Oregon, USA

Byron Marshall
College of Business, Oregon State University, Corvallis, Oregon, USA

Forough Nasirpouri Shadbad
College of Business, Oregon State University, Corvallis, Oregon, USA

Sanghyun Hong
School of Electrical Engineering and Computer Science, Oregon State University, Corvallis, Oregon, USA

ABSTRACT

Security Operation Centers (SOC) play a key role in protecting organizations from many cybersecurity threats, such as system intrusion or information breaches. A major challenge in improving SOC operations is the adequacy of the data used to identify such threats. Detection tools employed by SOCs are largely based on observable *telemetry indicators* (e.g., network traffic patterns or system logs and activities collected from user devices) (Bryant and Saiedian 2020). However, the use of such telemetry data without understanding human behaviors in-depth can lead to increasing false-positive alerts. Prior work shows that it can even be a more significant problem when analysts largely ignore alerts if they are overwhelmingly *false-positive* (Bryant and Saiedian 2020; Hindy et al. 2019; Sacher 2020). These *false positive alerts* raise SOC analysts' cognitive workload, diminish conscious cognitive processing, and decrease their trust in future alerts (Ayyagari et al. 2011; D'Arcy et al. 2014; Zhang et al. 2022).

In this work, we hypothesize that poor integration of human behavior models are the root-case of those false positives in SOC tools. It is widely believed that individual end-user mistakes, risky actions, and unauthorized actions are major contributors to security incidents and

[1] Corresponding author. curym@oregonstate.edu +1 541-737-3617

breaches (Verizon 2022). Behavioral security researchers have made significant theoretical contributions to understanding the drivers of information security policy (ISP) compliance/non-compliance. However, there is little evidence that these theoretical models can be incorporated in SOC operational tools. This is partly due to a lack of guidance for practitioners on how to incorporate constructs from these models in tools to mitigate risky behavior (Marshall et al. 2021). Practically speaking, one of the challenges in utilizing existing behavioral models is that there are many theories and each one has many survey items, which are simply not feasible to collect in an organizational context.

We propose a novel approach to address these challenges. First, we collect *telemetry indicators* from multiple organizational data sources which may be found in typical enterprise security tools to detect security incidents and breaches. Second, we develop a *subject matter experts'* consensus to better characterize the user-based riskiness of each indicator. Third, we identify a light weight set of *user behavioral indictors* of riskiness in Information Security Policies (ISP) compliance and combine it with a subset of the collected *telemetry indictors* to predict security incidents and breaches with fewer false positives in detection tools. Specifically, we ask the following research questions:

1. What *telemetry indicators* can we collect to identify risky user behaviors?
2. What *indicators* would, in the opinion of *subject matter experts*, increase the utility of cybersecurity operations?
3. Can we build *predictive human behavioral models* by combining a light weight set of *user behavioral indicators* of risk with the *telemetry indicators* we collect?
4. Do predictive *human behavioral models* reduce cognitive workloads for SOC analysts by *reducing false alerts*?

We seek feedback from the research community on our study design described below.

Task 1: Collect telemetry data of security incidents and breaches

We answer our first research question by partnering with an enterprise SOC that operates in higher education to collect telemetry network indicators of risky user behavior, e.g., clicking on phishing messages, having an account compromised, reporting junk and phishing messages, and participating in user security training, among others. Data was collected in support of research question 1, from enterprise security tools summarized in Table 1. Note that some data is aggregated cumulatively (e.g., total users), while other data is collected over a time span (e.g., daily or over a range of time). Using a computational data wrangling pipeline, we associated multiple telemetry risky behavior indicators with users. Linking users and devices is somewhat difficult since some devices support multiple users. A proxy based on the most frequent logins was an indicator of the most likely user of a device. Our data contains multiple flat files extracted from the telemetry sources. We anticipate the refreshing of this data can be automated and the time horizon adjusted to cover study lengths that range from one to six months. We store all data on a secure storage managed by the SOC. We anonymize users with a method in our pipeline to replace identifiable data with a unique identifier.

Table 1. Summary of the telemetry indicators of riskiness collected.

Source	Description	Data frequency
Devices	Includes laptops workstations and servers. Does not include mobile devices. In many cases a device can be somewhat linked to the most frequently used user	Cumulative
Users	Total accounts, many are inactive or do not access services	Cumulative
Active Users	Accounts being monitored	Daily
Domain names	Domains being monitored	Daily
Accounts compromised	Accounts which had to be reset due to clicking on phish, malware, password compromise or other issue	Multiple years
Risky users	A proprietary estimated risk score based on different mechanisms that are meant to elevate the risk level based on potential risk across a wide range of possible attacks, to include anonymous IP use, atypical travel, signing in from infected devices, signing in from IP addresses with suspicious activity, signing in from unfamiliar locations	Daily
Risky logins	atypical travel, signing in from unfamiliar locations	Daily
Software vulnerabilities	List of known software vulnerabilities	Cumulative
Devices with known vulnerabilities	Devices that have software installed which is known to have vulnerabilities	Cumulative
Reported spam or phishing	Suspected junk or phishing emails forwarded by users to IT for verification	30 days
Reported spam or phishing	Suspected junk or phishing emails flagged by users in their email client	30 days
User Security Training	Report of completion for required security training. All users are required to complete this training.	Cumulative
Other observable indicators?		

Task 2: Develop an expert consensus of user-based riskiness indicators

Prior work suggests that many of these telemetry indicators can highlight cybersecurity risks related to individuals. E.g., some SOC tools generate a proprietary user estimated risk score synthesized from multiple telemetry risk indicators. To answer our second research question, we propose to survey cybersecurity experts opinions on the importance of potential indicators to

identify risky behavior. We plan to solicit responses from security analysts, Chief Information Security Officers (CISO), behavioral researchers and IT auditors.

The importance of specific controls (e.g., patching, training, and email filtering) are largely driven by security processes rather than individual predispositions. Still, user choices do impact the effectiveness of such controls. Note that our survey focuses on the human element and not on which technical events are of the most concern from an organizational perspective. We aim to identify which items in the opinion of experts, usefully indicate a user's cybersecurity capabilities, mindset, or predilection. Put another way, to what degree do these indicate the likelihood that a user will effectively do (or not do) their part to help protect organizational systems from cyber threats? We also plan to ask about the efficacy of *user behavioral indicators* as well as telemetry indicators.

Expert Survey: In your expert opinion, how important would each of the following measures indicate that a user's predisposition is risk-laden (likely to comply or not comply) from a cyber security perspective? (5 choices from not at all important to very important).

Telemetry and Technically Observable Indicators:

- Count of how many times a user's account was reset based on some evidence of compromise
- Resources controlled by the user's account was used to host phishing infrastructure
- The frequency and type of login attempts noted for the account
- The quantity of malware found in emails received by the user
- A system-assigned risk score
- The user flags suspicious emails to be reviewed as a possible phishing
- User completion of Security Education Training and Awareness (SETA)
- The presence of software with known vulnerabilities on the user's device
- The frequency that the user clicked on malicious links

Sociometric Indicators

- The user feels capable and empowered to take needed action (self-efficacy)
- The user believes their duties support/allow them to take needed cybersecurity actions (role theory)
- The user believes that policy driven activities will be effective in reducing risk (response efficacy)

- The user

The survey results will shed some lights on choosing indicators to for subsequent tasks. And, we may be able to interestingly compare the expert opinions against telemetry information to validate their expertise.

Task 3: Developing a predictive model by combining a light weight set of user behavioral indicators of risk with the telemetry indicators.

Prior work on behavioral security research focuses on developing psychometric-based theories to understand the antecedents of security compliance behavior, e.g., Protective Motivation Theory (PMT) (Boss et al. 2015; Johnston et al. 2015; Menard et al. 2017), the InfoSec Process Action Model (IPAM) (Curry et al. 2018, 2019), Technostress and Role-stress (Nasirpouri Shadbad and Biros 2021; Shadbad and Biros 2020), and Unified Model of Information Security Compliance (UMISC) (Moody et al. 2018). However, a major challenge in utilizing existing psychometric constructs in behavioral models is that there are many competing theories, and each one has many survey-based items in their protocol. Practitioners are rarely given guidance on which constructs are most important, and it is impractical to scale in an organizational context.

One promising approach is the use of *systematic feature selection* techniques to develop smaller subsets of items which have been shown to provide meaningfully indicative power on IPAM (Marshall et al. 2021), and more recently on Technostress and Role-stress models (Marshall et al. 2022). These studies add support to a growing body of evidence that a feasible (shorter) list of indicators can provide predictions of sufficient power that also align with theory driven behavioral drivers of non-compliance behavior.

To answer our third research question, we continue the prior work's directions and employ *systematic feature selection* techniques for building *predictive human behavioral models* by combining a light weight set of *user behavioral indicators* of risk with the *telemetry indicators* we collect. One aspect still under investigation is deciding which theoretical behavioral models to operationalize? The *feature selection* technique's effectiveness has been shown using IPAM which is a process model for nudging participants towards a desired behavior (e.g. better information security policy compliance). We also consider incorporating Technostress and Role-stress, which theorize that uncertainty in one's role and the overwhelming complexity of IT are key drivers of ISP compliance/non-compliance to be highly applicable for our study. All three models are known suitable theories to the *systematic feature selection* technique and strong candidates. Additionally, the UMISC, which synthesizes eleven existing models is another candidate model whose efficacy we plan to evaluate for this study.

In our *pilot study* design, we plan to administer a survey of 100+ users. *Feature selection* efforts employing datasets from previous studies will be used to initially shorten the list of items and the pilot results should allow us to further winnow the list. Then working with the organizational IT in a *follow-on study* we plan to administer the survey more broadly. Once we are able to show the merits of our survey items, we may advocate for them to be added to Security Education Training and Awareness for users to complete annually to simplify future data collection and support our desire to integrate this data into the SOC tools.

Task 4: Determine whether predictive *human behavioral models* reduce cognitive workloads for SOC analysts by *reducing false alerts*?

To answer research question four, we aim to compare and contrast the predictive power of the *user behavioral indicators* and the *telemetry indicators* individually alongside the lightweight *predictive human behavioral models*. We theorize our synthesized model can result in more accurate predictions of risky behaviors as characterized by fewer false alerts. We also anticipate it would reduce cognitive workloads of SOC analysts.

In conclusion, this work in progress proposes a novel approach to building accurate predictive modes for identifying security threats by combine behavioral indicators and telemetry data. We first collect *telemetry indicators* from typical enterprise security tools. We then develop a *subject matter experts'* consensus that characterizes the user-based riskiness of each risk indicators. Using them as inputs, we finally employ *feature selection* and identify a light weight set of *user behavioral indictors* of riskiness in information security policies compliance plus *telemetry indictors* to improve the predictive power of SOC detection tools (fewer false positives). If successful, these efforts would be a significant contribution to advance the knowledge of how behavioral indicators can address cybersecurity threats to organizations by offering models that have higher security threat predictive power than current approaches while also reducing SOC analyst's stress.

ACKNOWLEDGEMENTS

This work was generously supported by University Information and Technology at Oregon State University.

REFERENCES

Ayyagari, R., Grover, V., and Purvis, R. 2011. "Technostress: Technological Antecedents and Implications," *MIS Quarterly: Management Information Systems*. (https://doi.org/10.2307/41409963).

Boss, S., Galletta, D., Lowry, P., and Moody, G. 2015. "What Do Users Have to Fear? Using Fear Appeals to Engender Threats and Fear That Motivate Protective Security Behaviors," *MIS Quarterly (*. (http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2607190).

Bryant, B., and Saiedian, H. 2020. "Improving SIEM Alert Metadata Aggregation with a Novel Kill-Chain Based Classification Model," *Computers & Security* (94). (https://doi.org/https://doi.org/10.1016/j.cose.2020.101817).

Curry, M., Marshall, B., Correia, J., and Crossler, R. E. 2019. "Infosec Process Action Model (IPAM): Targeting Insiders' Weak Password Behavior," *Journal of Information Systems* (33:3). (https://doi.org/10.2308/isys-52381).

Curry, M., Marshall, B., Crossler, R. E., and Correia, J. 2018. "InfoSec Process Action Model (IPAM): Systematically Addressing Individual Security Behavior," *Data Base for Advances in Information Systems* (49:S1), pp. 49–66. (https://doi.org/10.1145/3210530.3210535).

D'Arcy, J., Herath, T., and Shoss, M. K. 2014. "Understanding Employee Responses to Stressful Information Security Requirements: A Coping Perspective," *Journal of Management Information Systems*. (https://doi.org/10.2753/MIS0742-1222310210).

Hindy, H., Brosset, D., Bayne, E., Seeam, A., and Bellekens, X. 2019. "Improving SIEM for Critical SCADA Water Infrastructures Using Machine Learning," *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* (11387 LNCS), Springer Verlag, pp. 3–19. (https://doi.org/10.1007/978-3-030-12786-2_1).

Johnston, A., Warkentin, M., and Siponen, M. 2015. "An Enhanced Fear Appeal Rhetorical Framework: Leveraging Threats to the Human Asset Through Sanctioning Rhetoric.," *MIS Quarterly* (39:1), pp. 113–134.

Marshall, B., Curry, M., Crossler, R. E., and Correia, J. 2021. "Machine Learning and Survey-Based Predictors of InfoSec Non-Compliance," *ACM Transactions on Management Information Systems*. (https://doi.org/10.1145/3466689).

Marshall, B., Shadbad, F. N., Curry, M., and Biros, D. 2022. "Do Measures of Security Compliance Intent Equal Non-Compliance Scenario Agreement?," in *Proceedings of the 17th Pre-ICIS Workshop on Information Security and Privacy, Copenhagen Denmark, December 11, 2022*.

Menard, P., Bott, G. J., and Crossler, R. E. 2017. "User Motivations in Protecting Information Security: Protection Motivation Theory Versus Self-Determination Theory," *Journal of Management Information Systems* (34:4), pp. 1203–1230. (https://doi.org/10.1080/07421222.2017.1394083).

Moody, G., Siponen, M., Quarterly, S. P.-M., and 2018, U. 2018. "Toward a Unified Model of Information Security Policy Compliance," *MIS Quarterly* (42:1).

Nasirpouri Shadbad, F., and Biros, D. 2021. "Understanding Employee Information Security Policy Compliance from Role Theory Perspective," *Journal of Computer Information Systems* (61:6), Taylor and Francis Ltd., pp. 571–580.

(https://doi.org/10.1080/08874417.2020.1845584).

Sacher, D. 2020. "Fingerpointing False Positives," *Digital Threats: Research and Practice* (1:1), ACM PUB27 New York, NY, USA . (https://doi.org/10.1145/3370084).

Shadbad, F. N., and Biros, D. 2020. "Technostress and Its Influence on Employee Information Security Policy Compliance," *Information Technnology & People* (35:1), Emerald Group Holdings Ltd., pp. 119–141. (https://doi.org/10.1108/ITP-09-2020-0610/FULL/XML).

Verizon. 2022. "Data Breach Investigations Report." (https://www.magonlinelibrary.com/doi/pdf/10.12968/S1361-3723%2822%2970578-7).

Zhang, Z., Patterson, Z., Hicks, M., and Wei, S. 2022. "99% False Positives: A Qualitative Study of {SOC} Analysts' Perspectives on Security Alarms," *31st USENIX Security Symposium (USENIX Security 22)*, USENIX Association. (https://www.usenix.org/conference/usenixsecurity22/presentation/zhang-zenong).