Blog Post

A key challenge in guaranteeing information security continuity, is enforcing conformity among interested parties. Conformity within this context relies largely on non-concrete, human-centric factors, such as trust in risk management processes and information security governance. In the case of trust, it is possible for that trust to become an attack vector, regardless of how many security practices are enforced. As an example of this phenomenon, a company may implement strong email filtering, causing a user to trust the system to the extent that they would comply with any malicious email that bypasses the filter, thinking that it is safe to follow (Pienta et al., 2020). The authors of the previous paper note that this "mindless compliance" poses a serious threat to information security, and suggest that conscious distrust should form part of any employee's standard practice, which could form a control objective, practically speaking. The findings of Donalds and Osei-Bryson (2020) corroborate this suggestion, as they found that general security awareness contributes to sustained compliance to internal security practices.

In addition, emerging practices can be leveraged to improve conformity. One such example is the use of predictive modeling. Addae et al. (2019) proved the viability of this approach by leveraging existing cybersecurity literature using a Bayesian Network to determine a user's security needs, and predict their behavior, based on a range of complex input variables (such as working times and working locations). Tubío et al. (2020) applied a similar approach to risk analysis, and used machine learning techniques to predict which digital business assets would carry the most risk (including risks caused by humans). This approach was further augmented by the novel use of future threat probabilities as opposed to historical data, which makes the resulting data more relevant to the systems in their current state. Although these technologies are in their infancy, companies may find it useful to begin collecting data regarding how individuals interact with their security controls, making it possible to use these predictive modeling techniques to improve compliance once they are refined, or use already established technologies to do the same.

References

Addae, J., Sun, X., Towey, D. & Radenkovic, M. (2019). Exploring user behavioral data for adaptive cybersecurity. User Modeling and User-Adapted Interaction. 29:1-50. DOI: http://doi.org/10.1007/s11257-019-09236-5

Donalds, C. & Osei-Bryson, K-M. (2020) Cybersecurity compliance behavior: Exploring the influences of individual decision style and other antecedents. International Journal of Information Management 51(C): 1-16. DOI: https://doi.org/10.1016/j.ijinfomgt.2019.102056

Pienta, D., Tams, S. & Thatcher, J. (2020) 'Can Trust be Trusted in Cybersecurity?', Hawaii International Conference on System Sciences 2020. Grand Wailea, A Waldorf Astoria Resort: Hawaii, January 7-10. ScholarSpace: Web. 4264-4273.

Tubío, P., López Bravo, C. & López, J. (2019) Improving information security risk analysis by including threat-occurrence predictive models. Computers & Security 88: 1-10. DOI: http://doi.org/10.1016/j.cose.2019.101609.