Title: Correlating Human Traits and Cybersecurity Behavior Intentions

Author: Margaret Gratian, Sruthi Bandi, Michel Cukier, Josiah Dykstra, Amy Ginther

PII: S0167-4048(17)30252-3
DOI: https://doi.org/10.1016/j.cose.2017.11.015
Reference: COSE 1242

To appear in: *Computers & Security*

Received date: 26-7-2017
Revised date: 10-11-2017
Accepted date: 20-11-2017

Please cite this article as: Margaret Gratian, Sruthi Bandi, Michel Cukier, Josiah Dykstra, Amy Ginther, Correlating Human Traits and Cybersecurity Behavior Intentions, *Computers & Security* (2017), https://doi.org/10.1016/j.cose.2017.11.015.

# Correlating Human Traits and Cybersecurity Behavior Intentions

Margaret Gratian[1], Sruthi Bandi[1], Michel Cukier[1], Josiah Dykstra[2], Amy Ginther[1]
The University of Maryland, College Park[1], Laboratory for Telecommunication Sciences[2]
College Park, Maryland, United States
{mgratian, sbandi, mcukier, aginther}@umd.edu, jdykstra@ltsnet.net

Biographical Sketches

Margaret Gratian is a researcher at the Department of Defense and a PhD student in Reliability Engineering at the University of Maryland, College Park. She has a B.S in Mathematics and Computer Science from the University of Maryland. Her research interests include evaluating and quantifying user cyber security behaviors and user susceptibility to cyber crime.

Sruthi Bandi is a quantitative data analyst who uses business analytics to influence IT investment decision making. She holds a master's degree in Information Management and a bachelor's degree in Computer Science. She has conducted research on human behavior and information systems in the domains of health care and cyber security at the University of Maryland, College Park. She is a former software engineer and has experience developing simulators and optimization systems for thermal power plants.

Michel Cukier is an associate professor of reliability engineering with a joint appointment in the Department of Mechanical Engineering at the University of Maryland, College Park. He is also the director for the Advanced Cybersecurity Experience for Students (ACES). His research covers dependability and security issues. His latest research focuses on the empirical quantification of cybersecurity. Dr Cukier has published more than 70 papers in journals and refereed conference proceedings in those areas.

Josiah Dykstra holds the PhD degree in Computer Science from the University of Maryland, Baltimore County. Dr Dykstra is a Senior Researcher at the Laboratory for Telecommunication Sciences in College Park, MD. His research interests include network security, digital forensics, cloud computing, and human resilience in cybersecurity including augmented reality. He is a Fellow of the American Academy of Forensic Sciences and member of ACM.

Amy Ginther is an IT Specialist at the University of Maryland where she directs Project NEThics, a Division of Information Technology, Security Office group charged with promoting acceptable use of information technology and addressing misuse incidents. She supports student researchers in puzzling out ethical practice issues and administrative challenges. Usable security is a primary research interest area, including improving organizational practice through data driven decision making. Ms Ginther holds an M.Ed. from the University of Vermont and worked in residential life and student conduct/academic integrity roles before moving into IT.

***Abstract*— In this paper, we correlate human characteristics with cyber security behavior intentions. While previous papers have identified correlations between certain human traits and specific cyber security behavior intentions, we present a comprehensive study that examines how risk-taking preferences, decision-making styles, demographics, and personality traits influence the security behavior intentions of device securement, password generation, proactive awareness, and updating. To validate and expand the work of Egelman and Peer, we conducted a survey of 369 students, faculty, and staff at a large public university and found that individual differences accounted for 5-23% of the variance in cyber security behavior intentions. Characteristics such as financial risk taking, rational decision-making, extraversion, and gender were found to be significant unique predictors of good security behaviors. Our study revealed both validations and contradictions of related work in addition to finding previously unreported correlations. We motivate the importance of studies such as ours by demonstrating how the influence of individual differences on security behavior intentions can be environment specific. Thus, some security decisions should also depend on the environment.**

***Keywords—human factors; individual differences; cybersecurity behaviors; cybersecurity intentions; surveys***

## I. Introduction

The human is often identified as the weakest link in cyber security, since any technical security solution is still prone to failures caused by human error. As such, there is a considerable amount of research that seeks to better understand users and the factors that influence their security behaviors. Though several researchers have identified