**TREO**
Technology, Research, Education, Opinion

# A Research and Teaching Platform for Attack and Defense in ERP systems

## Extending ERPsim research to study cyberattack motivations and detection

Michael Bliemel <Michael.Bliemel@OntarioTechU.Ca>, Bih-Ru Lea <leabi@mst.edu>, Lawrence Fredendall <flawren@clemson.edu>, Khalil El-Khatib <khalil.el-khatib@OntarioTechU.Ca>

Cybersecurity has become increasingly an important topic for IS research and education as adversaries become more sophisticated and attacks become more frequent (Wang et al., 2019). Often cyberattacks happen through internal systems access, either by insiders or compromised employee credentials (Bell et al. 2019). As almost all companies are operating on an Enterprise Resource Planning system (ERP), this research and teaching platform aims at studying motivations and behaviors of cyberattacks and defenses on a live ERP environment.

This study models cyberattack and defense on an ERP system using a marginal return function for cybersecurity investment, incorporating cyberattack options at various cost, risk, and penalty levels, and adopting machine learning and visual analytics utilizing Standard Operation Procedures (SOPs) (De Treville, et al., 2005). Individual and team motivations and behaviors are examined using personality traits (Lea, et al., 2019a, 2019b), cognitive aptitude (Lea, et al., 2017), and leader intervention (Hackman & Wageman, 2004).

The ERPsim simulation game in an in-memory SAP S/4HANA ERP system environment is used in this study as it has been widely used by prior literature to investigate Business Process Integration, decision making, IT adoption, team and user perceptions, and learning outcomes (Cronan & Douglas, 2012;Chronan, et al., 2011; Lea & Eng, 2019). Studies have reported that SOPs results in output consistency, efficiency, and learning rate of a given process and that SOPs may have influence on employee intrinsic motivation and creativity (De Treville, et al., 2005). The simulation scenario will facilitate the generation of SAP transaction data that can be used to train classification models to detect possible intrusions based on SOPs. Trained classification models as well as visual analytics of transactions/operations can be used to build dashboards with real time alerts for intrusion detection systems. These in turn can be used in subsequent simulations adding to a rich cybersecurity learning environment that combines both technical and game theoretic elements.

Apart from an engaging educational experience for learners, this scenario will enable research exploring individual personality traits, cognitive aptitude, and factors that impact learning and attitudes towards cybersecurity and ERP as well as team-based behavioral studies as to the motivations of why, when and how they would choose to carry out cyberattacks against other teams by accessing their login credentials to perform acts of sabotage.

**References: available upon request**