To report or not to report?

Extending Protection Motivation Theory to Vulnerability Discovery and Disclosure

Andrew William Green, Ph.D.

DeJarvis Oliver, Ph.D.

Amy B. Woszczynski, Ph.D.

KENNESAW STATE UNIVERSITY
COLES COLLEGE OF BUSINESS
Department of Information Systems and Security

Disclaimer

- The research presented here is the work of the authors and does not necessarily represent the views of Kennesaw State University or the University System of Georgia

KENNESAW STATE UNIVERSITY
COLES COLLEGE OF BUSINESS
Department of Information Systems and Security

Introduction

- Cybercriminals are motivated by financial gain from exploiting vulnerabilities, highlighting the urgent need for vulnerability discovery and remediation.
- Vulnerability researchers play a crucial role in identifying vulnerabilities, but they face a dilemma in deciding whether and how to report their findings.
- Vulnerability disclosure policies (VDPs) offer a potential solution by providing a safe and structured reporting mechanism.
- However, the adoption of VDPs by organizations remains limited, leaving researchers uncertain about potential legal repercussions and organizational responses.

KENNESAW STATE UNIVERSITY
COLES COLLEGE OF BUSINESS
Department of Information Systems and Security

Introduction

- Protection Motivation Theory (PMT) is proposed as a framework for understanding vulnerability researchers' decision-making processes.
- This study aims to adapt PMT to the context of vulnerability disclosure, exploring how factors like fear, rewards, and efficacy influence reporting intentions.
- The study will examine the influence of both personal and organizational threat appraisals on researchers' willingness to report.
- By understanding these factors, the study seeks to contribute to the development of effective VDPs and promote a culture of trust between organizations and vulnerability researchers.

KENNESAW STATE UNIVERSITY
COLES COLLEGE OF BUSINESS
Department of Information Systems and Security

Background

Laws, Regulation, and Retaliation

- Current US laws regarding cybersecurity, especially the CFAA and DMCA, are viewed by researchers as restrictive and inhibiting good-faith vulnerability research.
- Vulnerability researchers face risks of retaliation, including lawsuits and criminal charges, when reporting findings, especially concerning intellectual property.
- The US DOJ has attempted to clarify guidelines, but concerns remain about the definition of good-faith research and potential for civil claims.

Vulnerability Disclosure Policies

- VDPs offer a potential solution by providing a structured reporting mechanism and potential protections for researchers.
- However, VDP adoption remains limited, and the effectiveness of safe harbor provisions can vary.

KENNESAW STATE UNIVERSITY
COLES COLLEGE OF BUSINESS
Department of Information Systems and Security

Background

Protection Motivation Theory (PMT)

- PMT is a model that explains how fear appeals, threat appraisals, and coping appraisals influence behavior.
- It has been used in information security to promote employee compliance with cybersecurity guidelines.

Vulnerability Discovery and Disclosure (VDD) Model

- The VDD model adapts PMT to the context of vulnerability disclosure, focusing on how fear, rewards, and efficacy influence reporting intentions.
- It explores both personal and organizational threat appraisals and how they impact researchers' willingness to report.

KENNESAW STATE UNIVERSITY
COLES COLLEGE OF BUSINESS
Department of Information Systems and Security

Methodology

Expert Panel Review

- An expert panel consisting of two experienced vulnerability researchers and two cybersecurity academics was consulted to refine the survey instrument before distribution.

Power, Sample Size, and Effect Size

- Using effect sizes from prior studies, a sample size of 30-130 respondents was estimated to be sufficient for detecting effects.
- A target sample size of around 100 respondents was set.

Survey Distribution

- The Vulnerability Discovery and Disclosure (VDD) survey was disseminated using a 7-point Likert scale in Qualtrics.
- Survey items were modified from previously established scales where possible, but the survey was primarily exploratory.

KENNESAW STATE UNIVERSITY
COLES COLLEGE OF BUSINESS
Department of Information Systems and Security

Data Analysis

Invalid Data Resolution

- Survey bots were detected based on suspicious response patterns and timestamps.
- Data validation measures were implemented, including attention checks, completion rates, response times, and email validation.
- The final sample size after cleaning was 196 participants.

Respondents

- Respondents were US-based vulnerability researchers with diverse educational backgrounds, primarily holding 4-year degrees.
- The majority of respondents were White, male, and had an average age of 32.4 years with 7.1 years of experience in the field.
- The sample's representativeness was evaluated by comparing it to national statistics, revealing potential limitations in terms of race and ethnicity representation.

KENNESAW STATE UNIVERSITY
COLES COLLEGE OF BUSINESS
Department of Information Systems and Security

Data Analysis

Analytical Approach

- Harman's single-factor approach was used to test for common method bias (CMB), which was not found to be a significant issue.
- Principal components analysis (PCA) was employed for exploratory analysis and dimension reduction.

Principal Components Analysis

- PCA with varimax rotation resulted in 11 components explaining 74.613% of the total variance, exceeding the recommended threshold.
- Items were retained or dropped based on loadings, communalities, and Cronbach's alpha values, ensuring reliability and validity.
- Threat appraisals, coping appraisals, fear, and protection motivation intentions were analyzed separately, leading to the identification of a higher-order efficacy construct.

KENNESAW STATE UNIVERSITY
COLES COLLEGE OF BUSINESS
Department of Information Systems and Security

Results and Discussion

Threats

- The study found that vulnerability researchers do consider the potential harm to the organization (PSE-O) when deciding whether to report a vulnerability.
- This is a novel finding, as previous PMT research has primarily focused on personal threat appraisals (PSE-R).
- The results suggest that organizational threat appraisals are a significant factor in vulnerability disclosure decision-making.

Fear

- The study emphasizes the importance of reducing fear among vulnerability researchers to encourage reporting.
- Well-crafted VDPs, coordinated vulnerability disclosures, and safe harbor provisions can help alleviate fear and promote a culture of trust.
- Organizations should adopt a cooperative approach and consider offering bug bounties to further incentivize reporting.

KENNESAW STATE UNIVERSITY
COLES COLLEGE OF BUSINESS
Department of Information Systems and Security

Results and Discussion

Adaptive Rewards

- Adaptive rewards, such as recognition and bug bounties, are crucial for encouraging vulnerability disclosure.
- Organizations should clearly outline these rewards in their VDPs to attract and motivate researchers.
- The study suggests that well-defined VDPs can provide a sense of safety and increase the likelihood of reporting.

Efficacy

- The study found that self-efficacy and response efficacy combine to form a higher-order construct of perceived efficacy.
- This suggests that vulnerability researchers need to believe in their ability to report effectively and that their reports will be taken seriously.
- Organizations can enhance perceived efficacy by providing clear guidelines, points of contact, and assurances of protection.

KENNESAW STATE UNIVERSITY
COLES COLLEGE OF BUSINESS
Department of Information Systems and Security

Conclusion

Overall Conclusion

- This exploratory study analyzed how vulnerability researchers decide whether to disclose vulnerabilities, creating the VDD model based on modified PMT.
- The VDD survey was refined to 68 items through a rigorous process.

Theoretical Contributions

- Efficacy emerged as a higher-order construct, suggesting future research on providing instructions and policies to increase researchers' disclosure likelihood.
- The study introduced organizational perspectives (PSE-O, PVU-O), which were retained in the PCA analysis, indicating their importance in decision-making.

KENNESAW STATE UNIVERSITY
COLES COLLEGE OF BUSINESS
Department of Information Systems and Security

Conclusion

Practical Contributions

- Organizations should reduce fear through well-crafted VDPs, outlining clear reporting processes and protection measures.
- Adaptive rewards and a sense of safety can encourage reporting, benefiting organizations by identifying vulnerabilities early.
- User-friendly VDPs, written in clear language, are crucial for fostering positive collaborations with vulnerability researchers.

Limitations and Future Research

- The study used self-reports, which may have limitations despite efforts to minimize them.
- The non-probabilistic sample and the survey bot attack, although addressed, are limitations.
- Future research should explore ways to block survey bots, conduct qualitative studies on researchers' experiences, and gather data from organizational employees involved in VDPs.

KENNESAW STATE UNIVERSITY
COLES COLLEGE OF BUSINESS
Department of Information Systems and Security

Thank you!

- This presentation is available for download at https://andygreen.phd/presentations

- Email – andy.green@kennesaw.edu

KENNESAW STATE UNIVERSITY
COLES COLLEGE OF BUSINESS
Department of Information Systems and Security