

Thesis Project Portfolio

Securing A Moral Distress Reporting and Analysis System With A Role-Based Access Control Approach
(Technical Report)

Ashley Madison Data Breach of July 2015: Determining Moral Responsibility with Actor-Network Theory and Conditions of Responsibility Framework
(STS Research Paper)

An Undergraduate Thesis

Presented to the Faculty of the School of Engineering and Applied Science
University of Virginia • Charlottesville, Virginia

In Fulfillment of the Requirements for the Degree
Bachelor of Science, School of Engineering

Neha Krishnakumar

Spring, 2024

Department of Computer Science

Table of Contents

Sociotechnical Synthesis

Securing A Moral Distress Reporting and Analysis System With A Role-Based Access Control Approach

Ashley Madison Data Breach of July 2015: Determining Moral Responsibility with Actor-Network Theory and Conditions of Responsibility Framework

Prospectus

Sociotechnical Synthesis

The relationship between my technical and STS research projects involves the technical element of cybersecurity, and the STS element of Actor-Network Theory and the Conditions of Responsibility framework. The technical and STS research projects build from the technical and STS elements together, meaning that both are densely interconnected. The connection between my technical research project and cybersecurity is that the project seeks to develop a role-based access control (RBAC) implementation for a moral distress reporting system featuring sensitive data. As access control, a subset of cybersecurity is involved, this connection exists. There also exists a connection between my technical project and Actor-Network Theory and the Conditions of Responsibility framework, as I end up exploring the relationship between various actors that lead the moral distress reporting system, such as the Moral Distress Consultancy Service and the Research Team, and the powers these actors should hold in the system, which follows the Conditions of Responsibility framework were anything to go awry in my development of the security implementation. As for the STS research project, I analyze a case built on cybersecurity fundamentals and additionally apply the framework of Actor-Network Theory and the Conditions of Responsibility to the case. Thus, both technical and STS connections are fulfilled for my technical and STS research projects.

My technical project involves the development of a role-based access control implementation for an existing moral distress reporting system at the University of Virginia. I developed this role-based access control implementation with Amazon Web Services (AWS) CloudFormation, specifically with Yet Another Markup Language (YAML) template code, and with Sceptre. This automation tool enables me to generalize my code so I do not have to hardcode any values to give rise to vulnerabilities. Sceptre also drives the management of CloudFormation templates for security-based code. Development existed in iterations, as I

learned how each tool worked and explored the documentation sources for each tool. A proof-of-concept was first developed using the AWS console, and then code was written. After this, the code was deployed and tested and will continue to be evaluated in clinical trials in May.

My STS research project examined the case of the July 2015 breach of Ashley Madison, a site that allows its users to commit extramarital affairs. I analyzed the breach through the conceptual framework of Actor-Network Theory, which enumerates actors in a network framed by a network builder to examine the role that both human and non-human entities play, and the Conditions of Responsibility framework, which examines moral responsibility of an actor based on four conditions: wrong-doing, causal contribution, foreseeability, and freedom of action. Through my analysis, I deemed Ruby Corp, the owner of Ashley Madison, morally responsible for the breach, along with The Impact Group, which penetrated the system.

There was immense value in developing the code for my technical project and the analysis for my STS research project. The code for my technical project inspired me to become more interested in making better security-related code in the future, and secure a system with more quantifiable results. The analysis that I conducted for my STS research project made me interested in the ethics, business, and legal realm associated with the right to be forgotten and other socioethical frameworks, not just the frameworks I learned in class. The added domain of healthcare for my technical project, and sexuality for my STS research project, made me realize the requirement of cybersecurity in sensitive domains and how I would deeply look forward to working with either domain for a cybersecurity-related endeavor as a security engineer in the future.