Rudorwamwari Nyakanda

DRAFT DATE: Mar 23 2018

Center for Integrative Studies (CIS):

INDIVIDUAL MAJOR PROPOSAL:

CYBERSECURITY: Socio-Behavioral Components

1500 ST. OLAF AVENUE, NORTHFIELD, MN 55057

(619) 757 0732

rudonyakanda@gmail.com

nyakan1@stolaf.edu

Working Title: Cybersecurity: The Socio-Behavioral Components

Individual major advisor: Dr. Chuck Huff

Major Consultant: Dr. Rosenbaum

Research Consultant: Kasia Gonnerman

Peer Reviewers: Lamar Gayles, Elizabeth Bergstrand

Date of FRC: 3/9/18

Table of Contents:

- Individual Major Description
- Proposed courses
- Key questions asked
- Other relevant courses
- Senior Capstone Ideas
- Rationale

Description

Through the Socio-Behavioral Components of Cybersecurity major, I plan to explore aspects of human social-behaviors surrounding cybersecurity that affect online security. Initially, I intend to study the human psychology to understand components that could influence online negligence which results in security breaches. Living in a progressive technological world where all information is saved online, the government and corporations are at risk of cyber breaches. Although these acts of breaches are done online, humans are responsible for these malicious actions and therefore it would be fitting to study the social behaviors of both the user and the perpetrator. By exploring and studying online social behaviors, the government and corporations can always be a step ahead of the perpetrators by removing another limitation on cybersecurity.

My research into this field in the past three years has revealed that a lot of cooperation breaches happen through many possible ways including employee negligence from malicious intent or from innocent mistakes. Although, these companies may think they compensate their employees well in terms of pay and trainings in return for compliance and loyalty, they find themselves vulnerable to these cyber attacks. Therefore, by understanding the psychology behind human behavior and the human social traits, I will be able to use that information to understand the reason why individuals, corporations and governments may be at risk online. As a result, I'll be able to offer future directions that individuals, corporations and governments can take to mitigate online security risks.

Some of the questions that were explored in the construction of this major involves what company networks can and must do differently to minimize hackings. How effective are staff trainings on

security? The question of whether users are ever safe enough, raises the question of the extremities of online security that I'd be interested in exploring. For this major, I plan on taking classes from Psychology, Anthropology,Philosophy, Political Science and Computer Science to gain a holistic and engaging understanding of the effect human behavior has on security assurance. I am hoping these classes will equip me effectively on some researching and studying methods for ways to combat these breaches as well. Although a Computer Scientist could enter the field of Cybersecurity, I believe a different approach of studying the social behaviors of humans other than constantly programming firewalls would be the missing puzzle in the fight against cyber attacks.

Courses

Underlined classes have been taken or currently being taken

- Understanding social behaviors:

These courses will help me understand the fundamentals in human behavior and how humans interact with their different surroundings depending on their different background circumstances. I will be focusing on behavior that is influenced by malicious or negligent behavior. These six classes would assist in the core design of this major, as psychology is interdisciplinary and can be used to cross reference from other subjects like philosophy or anthropology. Human behavior in these two subjects is studied and analyzed critically and in different scopes from Psychology. It would be ideal to study at different angles to gain perspective.

- **SOAN 128 : Introduction to Cultural Anthropology**

  This class is influential in studying human behavior but with a cultural and social background. Besides being a prerequisite for the Global Interdependence class, it plays a role in laying down the fundamentals of social behavior through a different lens. This class will assist in understanding the fundamentals of social behaviors of internet users and how their different social backgrounds might influence how they use online devices.

- **SOAN 262: Global Interdependence** Vivian Choi (Spring 2019)

  This class studies different disasters across the globe, and how this affects our human nature as a result and how we choose to interact with each other. Although this class is not focused on hacking disasters, it will put into perspective the issues internet users face

after a security breach. For example, how does the world deal with hacking disasters?

- **Psych 249** : **Social Psychology** (FALL 2018)

  The scientific study of how people's thoughts, feelings, and behaviors are influenced by the actual, imagined, or implied presence of others. This class will build a bridge between the independent Study with Chuck Huff studying the socio-behavioral aspects of security, to an independent research extending on that particular study. Atleast, three psychology classes are needed for a level 300 Independent Research. Therefore, this class would be a perfect choice to expand my current studies in the Independent Study of the Behavioral Information Security.

- **Psych 221 Menacing Minds** (Interim 2018)

  This class will focused on studying and understanding criminal minds, and why they break the law. This class will be beneficial in understanding deviant behaviors i.e of those online users breaking the law. Studying human behavior is the core of this major and hence this class has laid a great foundation for my future studies of human behavior in Philosophy and Psychology.

- **Psych 391 Psychology of Good and Evil** (Spring 2019)

  This class will study the psychology of bad versus good. As I am studying the potential future directions of behavioral information security, it will be beneficial if I understood how humans decide to do bad or good things. This class would also give me skills in studying human behavior that would assist in the course of this major.

- **Psych 298 (IS: Behavioral Information Security Prof. Chuck Huff** (Spring 2018)-Current

  This independent study will focus on studying and understanding the behavioral information security. It will be the first step to researching the behavioral components of cybersecurity.

● Computer Programming:

The actual coding would assist in understanding how the software runs, how a computer can and should be protected. These classes will prepare me to gain language experience that would help me prepare for my career in cybersecurity.

- **125 CS for Science and Maths:**
  This class is an entry level for coders. We learn to primary coding languages R and Python. The latter is still commonly used in most organisations.

- **251 Software design**
  In Software Design class, coders are taught how to design their own software from

scratch. More advanced coding experience is achieved.

- **CS 263 Ethical Issues in Software Design Chuck Huff -Current**
  This class focuses on the ethics in designing software. This class would undoubtedly assist in future independent studies and or research. Understanding the ethics of computer usage would help me evaluate how our current policies and laws in the United States work. I would also be able to apply my knowledge based in ethics in my independent study with Dr. Kathryn Swanson studying the ethics in the cyberculture in the workplace.

- **276 Programming Language:Algorithm (SPRING 2019)-auditing option**
  In most Tech companies, knowledge of Algorithms is referred, if not required on most job applications. Taking this class would be an advantage. This class is recommended by most jobs if one is to venture into anything to do with computer science. This class would be taken in the second semester of my senior year, therefore since my senior year schedule would be really busy I've opted to auditing the class. This would ensure I grasp fundamental concepts without putting any unneeded pressures.

● Laws, Policies, Regulations:

Having an understanding of the Laws, Policies and Ethics would be greatly beneficial. Within Cybersecurity, there are policies that are influenced by laws and vice versa which may not necessarily be ethical or to the advantage of online users

- **PSci 285 International Law-(Spring 2019)**

  This class would open avenues to learning about international laws that might touch the jurisdiction of cyber laws and policies. Learning about how these laws may have restrictions especially online where online users are all over the world might be useful.

- **Philosophy 253: Phil Law, Politics & Morality**

  This class studies the philosophy behind human nature: Why do humans act in a certain way and how do they interact with each other? How do laws interfere with human nature? Are these laws ethical? This class lays a good foundation for my independent study in Ethics of policies and laws of privacy in the US

- **Phil 298 (IS: WorkPlace Cyberculture Ethics Prof. Kathryn Swanson)** (SPRING 2018) -Current Class

  This independent study focuses on the security cultures in the workplaces. We will focusing on some Philosophy ethical tools that would enable me to effectively study workplace security ethics that could potentially harm or limit the security levels of the

company. This independent study will bring in an integrative perspective into the major, that focuses on the surroundings versus human behavior.

- **Other learning experiences**

CCNA CISCO SECURITY CERTIFICATION

To prepare myself for the profession in the Security industry, it is recommended to sit for the CISCO CCNA Security exam to ensure I have adequate skills and knowledge to work with the CISCO networks in the professional world. With a CCNA Security certification, a network professional demonstrates the skills required to develop a security infrastructure, recognize threats and vulnerabilities to networks, and mitigate security threats. The CCNA Security curriculum emphasizes core security technologies, the installation, troubleshooting and monitoring of network devices to maintain integrity, confidentiality and availability of data and devices, and competency in the technologies that Cisco uses in its security structure. This certification has to be renewed every two year. Therefore after obtaining funding from the Piper Centre through the Johnson Fund, I'll be planning on taking the exam by the end of this summer.

Key questions

- **What makes behavioral cybersecurity different from cybersecurity and of what is it comprised?**
    - Why are cybersecurity and information assurance important?
    - How have cyber attacks shaped US national security , Corporate Online Security and Intelligence Security Protection (ISP)?
    - What do behavioral/personality/attitudinal aspects contribute to cybersecurity?

- **How can human behavior affect cybersecurity?**
    - What influences deviant vs negligent cybersecurity threatening behaviors?
        - Situational Influences (e.g. Company Culture; individual situations; codes of conduct)
        - Personality/Character
        - Skill and Knowledge
        - etc.
    - What kind of training, hiring policies, situational constraints, etc. *can* corporations implement to increase cybersecurity?
- **What ethical obligations do corporations, employers, employees, clients contractors, etc. have regarding cybersecurity?**
    - What are the obligations and rights associated with each of these roles?
    - What are the best ways to talk about cybersecurity as a value to each of these roles?
    - What kind of training, hiring policies, situational constraints, etc. *should* corporations implement to increase cybersecurity

- **How do we prepare for the future of behavioral cybersecurity?**
    - How might the roles mentioned above change in the future? For instance, with the evolution of Artificial Intelligence.
    - How will people, roles, and technologies in corporations change in the future?

Other relevant courses

1. **Prerequisites:**

a. **Introduction to Psychology** (Prerequisite for any Psychology classes)

This class has the fundamental principles to understand and study scientific thought or behavior. It is also a prerequisite to all future Psych classes. This class would be fundamental in giving me a baseline to studying "Menacing Minds", a criminal psychology class. How do hackers think and why do they do what they do?

Mathematics: Gateway to Understanding Computer Science

These courses are substantial because according to the John Hopkins University, one of the few accredited universities that offer a Masters and a PhD program in Cybersecurity, they require that students have at least these specific subjects to understand concepts in upcoming Computer Science and Psychology courses. I'm looking into joining John Hopkins for my Masters Program, and therefore it would be beneficial if I had these prerequisites.

a. Linear Algebra

b. Calculus 1

Senior Capstone Projects

1. Social Media Security Campaign (SMCOS)

This Social Media Campaign would be designed to reach college students with motivational messages and to communicate necessary skills for internet use while using their computers and cellphones. The aim of this campaign would be to spur students to an offline gathering place that educates students on practical online habits that prevent potential online breaches from occuring. This campaign would involve preliminary research on college student behavior online and viable ways to grab their attention online for educational purposes. From this information, a program would be created to educate the students on safe online practices.

A phishing study conducted at St. Olaf last Spring shows that freshmen were three time more likely than seniors to respond to a fake email trying to steal private information. Fully one quarter of first year students succumbed to the phishing attack. By leveraging the social pressures that college students experience online, the SMCOS would utilize social media platforms to educate students on better online practices. The social media platforms include and are not limited to Facebook and Instagram. By using classic social-psych principles drawn for the literature in the principles of attitudes and persuasion, we should be able to change students' behaviors and habits online. These two social-psych principles will assist in developing a better approach with the campaign. We will combine these principles with current literature in social media campaigns to make a lasting change in online habits by understanding the fundamental elements that can change human behavior in this new context. Researching college students'

online behavior would enable the campaign to capitalise on the students' attention by applying to their demographic and generational interests.

2. Designing Online Security Manuals & Testing

This project would be similar to the above campaign but dissimilar in the scale. The designed online security manuals would be tested on small focus groups and won't be implemented on the entire school like the previous one. These manuals would be available for the school to dispose to future college students and staff and would be available to the IT department.

3. IT Department Study & Analysis

This would be more of an internal research of the IT department security protocols and analyse them to my research on the best online practices. I would then analyse and evaluate if the IT department are being effective or doing more damage to the security infrastructure. If so, how can they change it for the better? This could also be used as the research component for the above projects.

Rationale

In the last decade, the Cybersecurity sector has increased in necessity due to the continuous advancement of technology. The 21st Century introduced us to digitization and the internet. The difference in the use of technology between the 20th and 21st century alone testifies how humans have become dependable on technology.

On campus alone students, professors and the administration spend at least 8 hours on technology combined, specifically computers and cellphones. As a result, this expansion in

human interaction with technology is guaranteed to cause problems. Due to this increased time online, a lot of criminal act has increased resulting in information being stolen and lost every minute. According to the *Identity Theft and Scam Prevention Services*, over 15 million United States residents have their identity lost every year and as a result over $50 billion worth of financials are lost or stolen.

Previously, a lot of Cybersecurity experts believed they could protect organisations and companies from breaches through coding an impervious and impenetrable firewall alone, but recent research has debunked this theory. Humans play a major role in the implementation of breaches and until organisations find a way to successfully train humans on the best safe online behavior, we have a long way to go. A firewall becomes "bulletproof" once the technology user religiously practices a guarded system online to ensure the loopholes in the firewall created by coders are not bypassed.

Studying the human social-behavioral components in technology will bridge the gap in the little knowledge currently available. I believe my major is a very strong concept because it is based off the liberal education system. The field of Cybersecurity involves an association of different subjects i.e Anthropology, Psychology, Computer Science and Philosophy to name a few. The Cyber World has a lot of laws, different human natures and types of crimes that are dealt with, therefore one has to be prepared to understand the different layers that come with the vicinity. Considering there aren't any majors of my kind offered at undergraduate level at any liberal arts college, this integrative aspect of my major will help foster an inclusive global engagement with the different professions in the world.

Personal Inspirations and Goals

According to *Cisco*, a multinational technology conglomerate,the field of Cybersecurity is the least populated. There is currently a shortage in employers in the field, firstly because the field is still new and expanding, and secondly there is an ongoing online cyber warfare to keep all information safe. My decision to create my own major in the Socio-Behavioral Components of Cybersecurity was influenced by the fact that there is a new field I could potentially academically learn from and contribute to as well. I first visited the Center for Integrative Studies during Week One of Freshman Year back in 2015. I was initially interested in Computer Science, but I had a deep curiosity in Cyber Security. When I asked Susan Carlson if I could turn my curiosity into a major, she was very encouraging. I first took Computer Science classes in my Sophomore year, and although I enjoyed coding, I didn't find the classes as quite mentally stimulating. A lot of my questions like "What are the limits of Computer Science?" , " How do humans interact with computers?" and " How can we implement Computer Science into our everyday life ethically?" were never answered, and I had to resort to my own research. During this initial research, I met Professor Huff who was the best expert in this field at St. Olaf. This is where my passion for Cybersecurity developed into a much bigger, meaningful and personal project: my independent major.

I believe my initial curiosity in technology was cultivated in high school at Arundel School in Zimbabwe. Most computer science classes were introduced to boys' schools only and leaving the science classes like Math and Physics to girl schools. The dominance of males in the technology field was reflected by the patriarchal system in my culture. Any career that was in this field was anticipated for men. My annoyance at this problem coupled with my intent in

taking coding classes have taken me this far. My choice to design my own major in a growing industry within the technology field itself is an empowering move for myself and all the women interested in the technology field. I'm hoping this independent major would be the first step to more academic researches I plan to take in the field of cybersecurity. I worked with the Network Administrator and the Information Security Specialist from the campus IT department in Summer 2017, and I got my first hands on experience in the field. I'm currently looking for Cyber Security internships, and so far, I've had interviews with Facebook, Amazon and Atlassian for their security intern positions.

After graduation, I'm hoping to apply to graduate programs to extend my knowledge in the field. I am currently eyeing the Rhodes Scholarship at Oxford, but I am also looking forward to possibly researching with the few experts in the field across the globe.

Summary of Consultations

Kasia Gonnerman

Kasia Gonnerman assisted with the researching skills that helped in the construction of the syllabus and the base of this proposal. She will continue to be available throughout her contract with St. Olaf.

Peer Review Group

Lamar Gayles '19 & Elizabeth Kathryn Bergstrand '19

I met with a peer review group that consisted of other individual majors on the third of May, 2017. Having individuals who were not experts in my field assisted in enunciating my proposal so that it appealed to everyone.

Mark Rosenbaum, Ph.D

In the primary construction of this major, I reached out to an academic expert in the fields of Cyber & Network Security, Information Assurance, Privacy, Information & Computer Ethics, Compliance & Governance (Policy). He also happened to be an associate of Professor Chuck Huff. Dr. Mark Rosenbaum is a Professor of cybersecurity and cyber ethics at the University of Maine at Fort Kent.