1. **Abstract** - Benefiting from the rewards of cyber systems comes with risks and associated potential costs. With quantified effectiveness and costs for various cyber defense tools and AnyLogic simulation software, this research focuses on modeling to determine the best combination of those tools.

2. **Motivation** - Cybersecurity breaches are a fact of life. How do you increase confidence and speed in deciding the best combination of cyber defense tools?

3. **Problem** - Cyber attackers have a growing number of ways they can degrade information confidentiality, integrity, and authenticity. The number of straight lines on Verizon’s 2016 Data Breach Investigations Report (DBIR) attack surface graph below depicts the different types of cyber attack reported to Verizon during 2015.

4. **Methodology** -
   a. Identify the cyber risks to defend against
      1) Refine the types of cyber attacks predicated on the organization and information to be defended
      2) Define the architecture to defend
   b. Based on the focus attack sequence determine for the impacted nodes the modeling elements
      1) Potential cyber defense tools
   c. Using AnyLogic software run simulations to determine effectiveness vs costs
      1) Built a model for each node that incorporates the effectiveness of cybersecurity tools
      2) Sequentially interconnect the nodes and associated cyber defense tools for the defined cyber attack and target
      3) Run the attack several time to determine the effectiveness of various solutions

5. **Results/Conclusion** - For a specified attack developed a working model and determined residual risk based on publicly available effectiveness for cyber defense tools. Statistical data will be required to improve model veracity.

6. **Current Work** - Developing a portfolios of models to support simulating several different types of cyber attacks and researching empirical cost and effectiveness data to improve the real world relevance of results.