

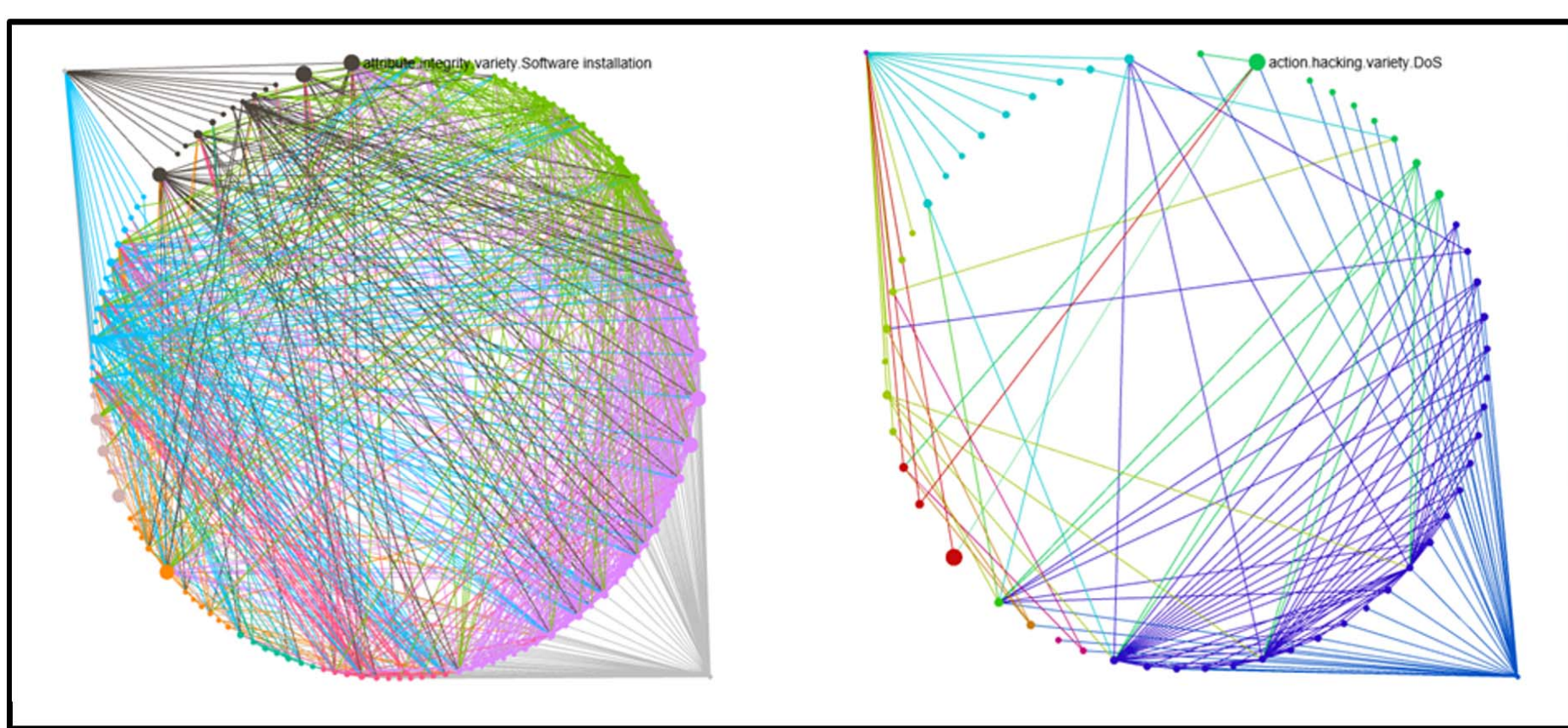
AnyLogic Modeling Cybersecurity Defense Effectiveness and Costs

J.E. Dietz, A. Gilbert, E. Hartman, R. Hilgers, S. Iyer, J. Lerums, L. Poe

1. Abstract - Benefitting 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?

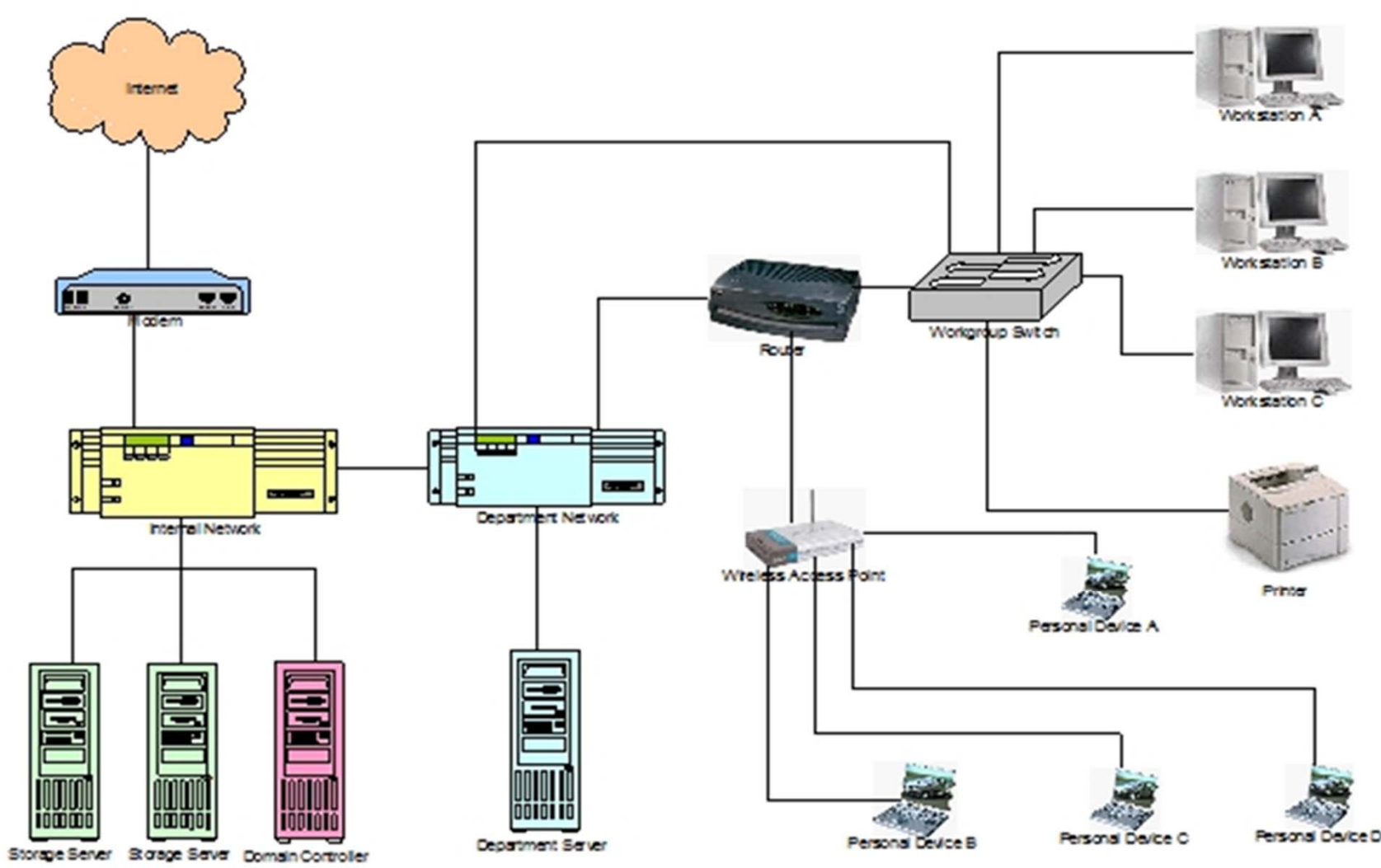
3. Problem - Cyber attackers have a growing number of ways they can degrade information confidentiality, integrity, and authenticity. The number of straight lines on Verizon's 2016 Data Breach Investigations Report (DBIR) attack surface graph below depicts the different types of cyber attack reported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



DBIR Attack Surface Graph Comparison Between "All Industries and Targets" (On The Left) and Education Services and "Medical, Payment, and Personal" information Targets (On The Right) (Verizon, 2016)

4. Methodology -

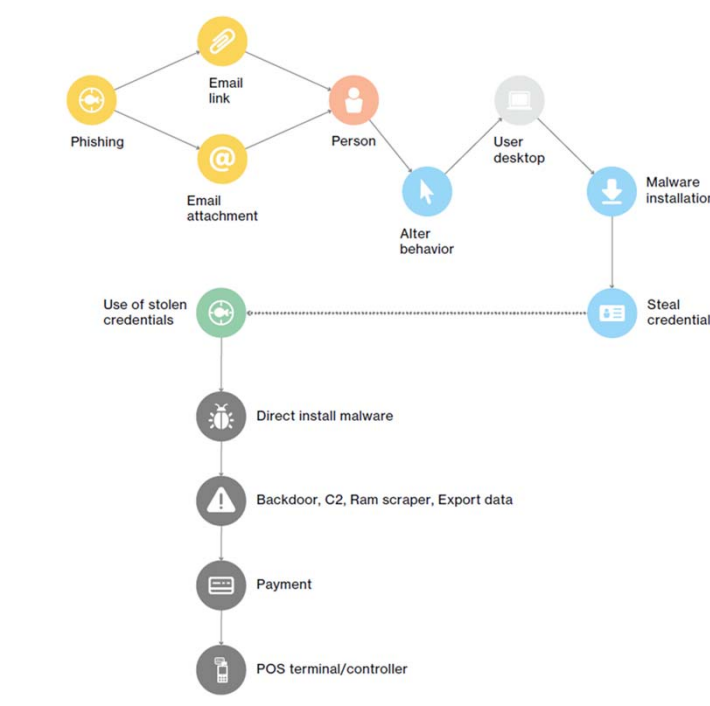
- a. Identify the cyber risks to defend against
 - 1) Refine the types of cyber attacks predicated on the organization and information to be defended
 - 2) Define the architecture to defend



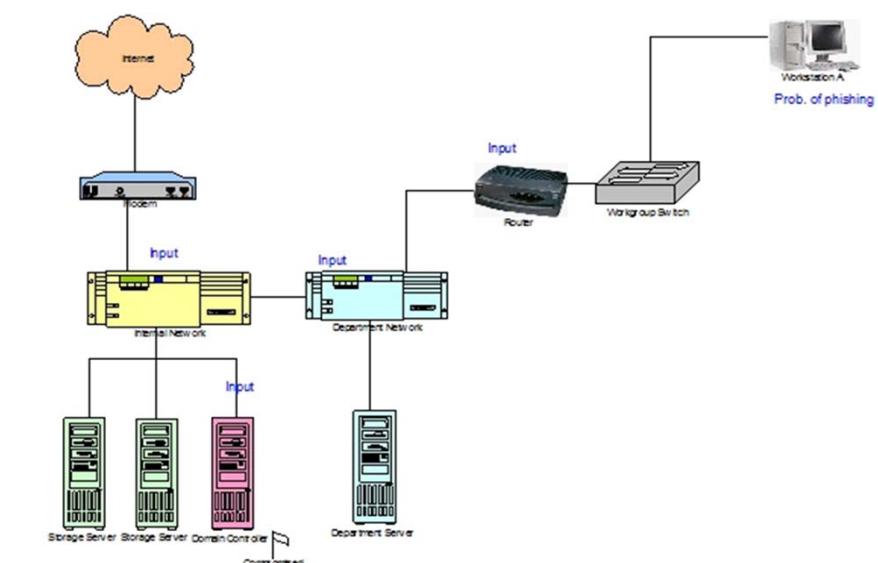
3) Analyze the architecture for potential attack sources and targets

Attack Sources	Attack Targets													
	Internet	Modem	Internal Network	Mail Server	Storage Server	Domain Controller	Department Network	Department Server	Router	WiFi Access Point	Work Group Switch	Work Stations	Printer	Personal Devices
Internet	High Risk													
Modem		High Risk												
Internal Network			High Risk											
Mail Server				High Risk										
Storage Server					High Risk									
Domain Controller						High Risk								
Department Network							High Risk							
Department Server								High Risk						
Router									High Risk					
WiFi Access Point										High Risk				
Work Group Switch											High Risk			
Work Stations												High Risk		
Printer													High Risk	
Personal Devices														High Risk

4) Based on cyber attack trends define the most likely type of attacks and targets



5) For each type of attack define the attack sequence and impacted nodes in the architecture.



b. Based on the focus attack sequence determine for the impacted nodes the modeling elements

1) Potential cyber defense tools

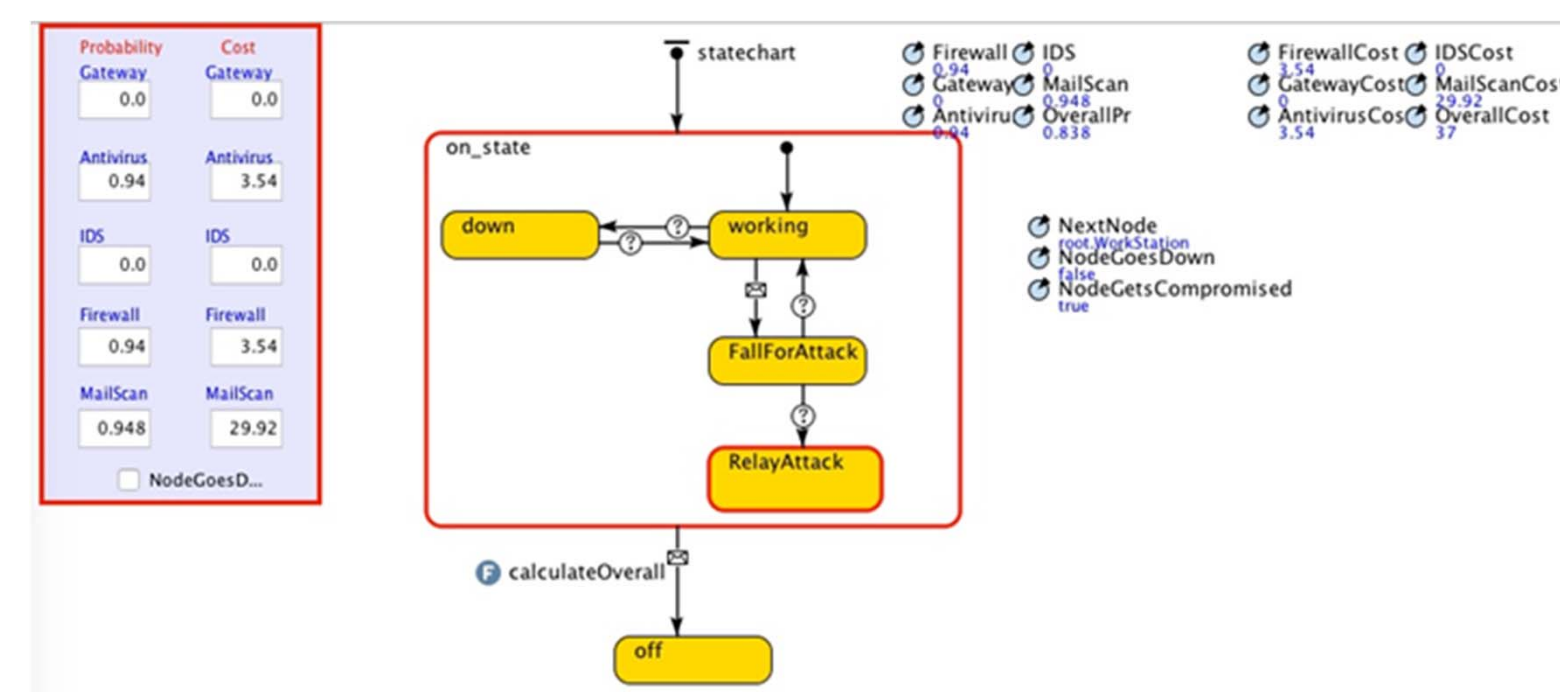
Device	Cybersecurity Tools					
	Antivirus (Symantec, McAfee, Avast, Avira, AVG, Avast, Avast, Avast)	IDS (Snort, Snort, Snort, Snort)	Firewall (Cisco, Cisco, Cisco, Cisco)	MailScan (MailScan, MailScan, MailScan, MailScan)	NextNode (NextNode, NextNode, NextNode, NextNode)	NodeGoed (NodeGoed, NodeGoed, NodeGoed, NodeGoed)
Internet	X	X	X	X	X	X
Modem	X	X	X	X	X	X
Internal Network	X	X	X	X	X	X
Exchange Server	X	X	X	X	X	X
Storage Server	X	X	X	X	X	X
Domain Controller	X	X	X	X	X	X
Dept. Network	X	X	X	X	X	X
Dept. Server	X	X	X	X	X	X
Router	X	X	X	X	X	X
WiFi Access Point	X	X	X	X	X	X
IDS Switch	X	X	X	X	X	X
Work Station	X	X	X	X	X	X
Printer	X	X	X	X	X	X
Personal Device	X	X	X	X	X	X

2) Effectiveness and costs of tools

Device	Cybersecurity Tool	Effectiveness	Cost
Internal Network	McAfee Endpoint Security	94.0%	\$ 3.54
Exchange Server	Sophos PureMessage	94.8%	\$ 29.92
Exchange Server	McAfee Endpoint Security	94.0%	\$ 3.54
Domain Controller	McAfee Endpoint Security	94.0%	\$ 3.54
Department Network	McAfee Endpoint Security	94.0%	\$ 3.07

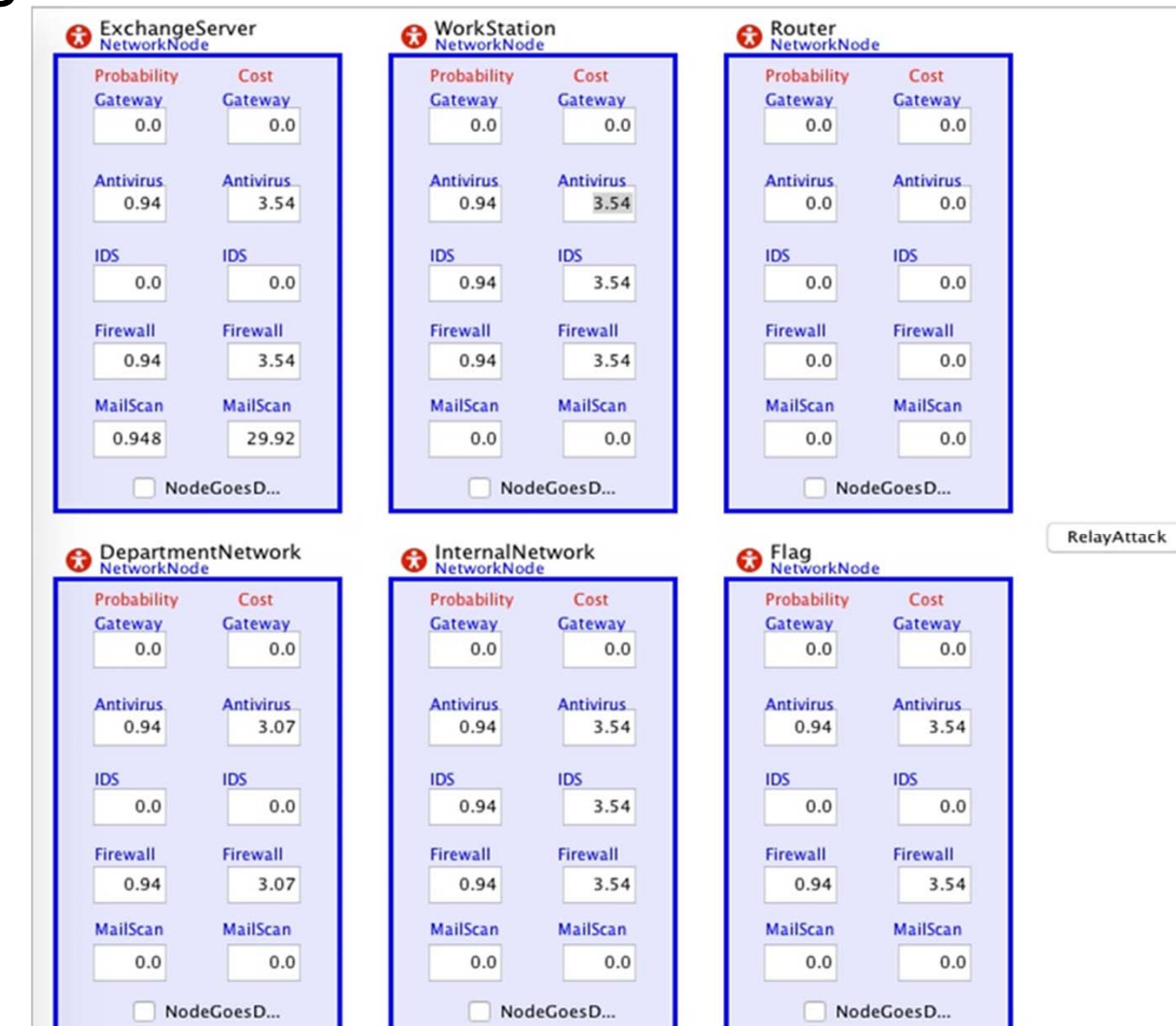
c. Using AnyLogic software run simulations to determine effectiveness vs costs

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.