**CYB 260 Module Project Three**

Douglas Few

Southern New Hampshire University

June 23, 2021

The partnership between Fit-Vantage and Helios comes with a number of security concerns that need to be addressed before any sharing of information occurs. In this brief, we will be focusing on two CIS controls to ensure that information security is responsibly upheld at all times. Namely, the two CIS controls being focused on will be 3.1 Run Automated Vulnerability Scanning Tools and 4.4 Use Unique Passwords.

Sub-Controls

The first sub-control that will be discussed is 3.1 Run Automated Vulnerability Scanning Tools. This is important because it will allow the network to automatically check for and detect vulnerabilities that would allow threats to breach the network and siphon customer health information. This should be implemented by installing the agreed upon Vulnerability Scanning Tool on every computer that connects to the network. Then, at scheduled times, the software will automatically perform a scan of the system to identify any potential gaps in security. The security team will then be notified and the issue will be dealt with.

The other sub-control that we will discuss is 4.4 Use Unique Passwords. This is important because it will minimize the potential damage in the event that an employee’s password is compromised by an aspiring attacker. This will be implemented by requiring all employees, administrative or otherwise, to create separate and unique passwords for every application or system that they have admissions for. This way, if an attacker were to intercept a password, they would only be able to gain access to one employee’s admissions on one particular system or application. This would minimize damage and allow the security team more time to detect the breach and stop the threat.

Necessity for Training Program

Training employees on the importance of security and how to deal with various security threats is critical to running a safe and ethical business. One of the most common security threats is phishing scams, in which an attacker will disguise their email address to appear legitimate and send a fake link that, when clicked on, grants the attacker access to the victim’s computer. If an employee at either Fit-Vantage or Helios were to fall for a phishing scam, the personal information of any or all of our customers could be compromised. In order to ensure the data security of our customers, I recommend we implement training programs for our employees that regularly focus on security awareness and avoiding these scams. This training would take place in two steps. The first step would be to develop a training regiment that is required for all employees that handle customer data. This training would occur in regular intervals, such as quarterly or bi-yearly, and would cover topics such as phishing scams and other social engineering topics to help raise employee awareness and educate on how to best counter these attacks. The second step would be to simulate phishing scams, send them to employees, and track their responses. This would not be in an attempt to punish or reprimand them, but rather to help them learn the importance of staying security-minded.

Outcome of Training

As a result of the training program outlined above, every employee of Fit-Vantage and Helios that handles or has access to sensitive customer information should be better prepared and knowledgeable in the event of an attempted security breach. This will allow both companies to remain trustworthy in the eyes of the consumer, which will likely lead to greater sales and prolonged business with current customers.