Anthony Gimei

Risk Assessment

Date of risk review: 8/26/2018

Compiled by: Anthony Gimei Date: 8/26/2018

Reviewed by: ………………………………… Date: …..…………..

Functionality/Activity: Risk Assessment

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Ref | The Risk: What can happen and how it can happen | The consequences of an event happening | | Adequacy of existing controls | Consequence rating | Likelihood rating  (1-5) | Level of Risk | Risk Priority |
| Consequences | Likelihood |
| 01 | Malware: Can infect a user’s computer and spread to the enterprise network. This can happen if a user visits a website and is deceived into installing the malware posing to be safe software. | Severe | Low | Daily antivirus and Malware scans. | Medium | 4 | 20% | 2 |
| 02 | DDoS: Customers and Employees unable to access website. Happens with site is flooded with artificial requests. | Severe | Low | Implement DDos detection and response tool | Medium | 1 | 10% | 4 |
| 03 | Phishing: Employee gives their credentials to a third party through a fake site from a link in an email | Moderate to Severe | High | Anti phishing campaigns. | High | 5 | 50% | 1 |
| 04 | Spyware: Used to monitor and send user information to 3rd parties. It can be installed via exploiting of existing vulnerabilities | Severe | Moderate | Install antispyware software. | High | 3 | 20% | 3 |