|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Risk:** | Analyze the risk associated with cyber criminals attacking our campaign material repository using ransomware to encrypt the data and locking out workstations. | | | | |
| **Risk Initiator** | *CEO raised concerns after reading about ransomware in the news.* | | **Threat** | *Nation State*  *Cyber Criminal*  *Organized Crime*  *Privileged Insider* | *Non-privileged insider*  *Hacktivist*  *Act of Nature*  *(Earthquake, Tornado, Flood etc.)* |
| **Asset at Risk** | *Campaign material stored on cloud storage.* | | **Impact Area** | *Availability*  *Confidentiality*  *Integrity* | *Safety*  *Compliance/Regulatory*  *…???* |
| **Risk Owner** | *Operations Manager* | | **Threat Type** | *Malicious*  *Accidental*  *Snooping*  *…???* | |
| **Forms of Loss** | *Productivity*  *Replacement*  *Response* | *Competitive Adv.*  *Reputation*  *Fines & Judgements* | **Key Controls** | Antivirus  Backup | |
| **Assumptions:** | * We treat ransomware as any other malware. * Ransomware encrypts the files and locks workstations. * Organization is not specifically targeted. * Organization will not pay ransom. * There is no free decryption tool available. * 50 workstations are critical for continuing to operate. | | | | |