HI David,

Owing to the recent security related incidents we have conducted a risk assessment. Here are the findings from our assessments.

Here is the risk identification and assessment report:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Asset** | **Category** | **Threat** | **Vulnerability** | **Asset Value**  **(1 to 4)** | **Threat value (1 to 2)** | **Vulnerability Value (1 to 2)** | **Overall Risk (1 to 16)** |
| Laptops | Hardware | Malware | Unrestricted Internet Access | $10,000 Financial Assets | Malware | Unrestricted Internet Access | Assign a numerical value to each threat, vulnerability, and asset based on its perceived severity and impact. |
| Internet access | Network | Data Breach | Lack of Security Policies | Data Assets | Data Breach | Lack of Security Policies and User Training | Assess the likelihood of each threat occurring and the likelihood of each vulnerability being exploited. |
| USB drives | Data | Insider Threat | Insufficient User Training | Hardware Assets | Insider Threat |  | Multiply the severity/impact value by the likelihood value for each threat and vulnerability. |
| Email system | Email | Social Engineering | Weak Endpoint Security | Email Assets | Social Engineering |  | Sum up the calculated values for all threats and vulnerabilities. |
| Financial assets | Transferred funds | Lack of Security Controls | Lack of Data Backup |  |  |  |  |
| Employees | pirated content | Reputation Damage | Inadequate Email Authentication |  |  |  |  |

On the basis of the above report, I would recommend……

Here is the risk-to-control mapping report:

|  |  |  |  |
| --- | --- | --- | --- |
| **Risk** | **Control** | **Features Required** | **Additional comments** |
| Risk of Malware Infections | The unrestricted internet access and the employee's use of uTorrent software to download pirated content introduces the risk of malware | Secure Internet Access | Security Culture: Building a strong security culture within the organization is crucial. This involves fostering a sense of responsibility and awareness among employees regarding cybersecurity best practices. |
| Risk of Data Breach | missing critical files on the laptops indicate a potential data breach or unauthorized access to sensitive information, | Endpoint Protection | Incident Response Team: Establish an incident response team composed of representatives from IT, security, legal, and management departments |
| Financial Risk | The organization experienced a financial loss of $10,000 due to the fraudulent email and unauthorized funds transfer. | Data Loss Prevention | Third-Party Risk Management: Evaluate and manage the risks associated with third-party vendors, contractors, or partners who may have access to the organization's systems or data |
| Reputation Risk | he lawsuit from Sony Pictures due to the employee's downloading of copyrighted content can damage the organization's reputation. | Regular Security Audits and Updates | Regular Security Assessments: Conduct periodic security assessments, including vulnerability scanning, penetration testing |

We are in process of identifying the products required for these controls. Here are the details of the shortlisted products.

|  |  |  |  |
| --- | --- | --- | --- |
| **Control** | **Product** | **Features available** | **Cost** |
| Internet Access Control: Implement a web filtering solution to block access to malicious or unauthorized websites. | Firewall | Firewalls help protect networks by monitoring and controlling incoming and outgoing network traffic, blocking unauthorized access and potentially malicious activity. | Implementing robust security solutions such as firewalls, endpoint protection, data loss prevention, and email security solutions may involve purchasing licenses |
| Endpoint Security Solutions: Deploy robust endpoint security solutions, including antivirus software, firewalls, and intrusion detection/prevention systems, to detect and prevent malware infections and unauthorized access to endpoints. | Antivirus/Anti-Malware Solutions | Antivirus software detects, prevents, and removes malicious software, including viruses, worms, Trojans, and other types of malware. | The cost may include developing training materials or enlisting the services of a third-party training provider. |
| Data Loss Prevention (DLP): Implement DLP measures to monitor and prevent unauthorized copying or transfer of sensitive data. This can include data classification, encryption, and monitoring of data exfiltration channels. | Endpoint Protection Platforms (EPP) | EPP solutions provide comprehensive security for endpoints, including desktops, laptops, and mobile devices. They often include features like antivirus, firewall, intrusion prevention, and data loss prevention. | Allocating resources to investigate the missing files, low memory issues, and the fraudulent email incident would involve the time and expertise of IT and security personnel. |
| Security Policies and User Training: Develop and communicate comprehensive security policies covering acceptable internet usage, software downloads, data handling, and incident reporting. Conduct regular security awareness training sessions to educate employees about cybersecurity best practices | Web Filtering Solutions | Web filters block access to malicious or inappropriate websites, preventing users from accessing harmful content and reducing the risk of downloading malicious software. | Conducting regular security audits, vulnerability assessments, and penetration tests to identify weaknesses and potential vulnerabilities |

Please let me know the additional details required.

Best Regards,

Rajan Kumar Sahu