| **IT Risk Scenario: Inadequate Patch/Vulnerability Management** | | | |
| --- | --- | --- | --- |
| 1. **Risk Scenario Description** | | | |
| **Risk Scenario Title** | Patch/vulnerability management process is inadequate to prevent incidents | | |
| **Risk Type** | 1-Product delivery; 2-Service quality; 3-Data and system protection | | |
| **Risk Scenario Category** | IT operations: Inability to provide reliable IT services because of operational IT mishaps | | |
| **Risk Scenario Reference** | 6D | | |
| **Risk Statement** | Inadequate patch and vulnerability management leaves systems vulnerable to attacks or crashes, reducing service levels. | | |
| **Risk Owner** | Portfolio manager/CIO/CTO/CDO | **Risk Oversight** | I&T Governance Board  Architecture Review Board  Steering Committee (Programs/ Projects)  Chief Risk Officer |

|  |  |  |  |
| --- | --- | --- | --- |
| 1. **Risk Scenario Components** | | | |
| **Actor/Threat Community** | Untrained/accidental insiders | | |
| **Intent/ Motivation** | The event is due to an enterprise insider and is deliberate but not malicious. The event may be caused by:   * Lack of understanding of enterprise approach and process to identifying, prioritizing and delivering IT-related changes * Lack of knowledge of requirements regarding current organization processes * Lack of training or awareness of the correct procedures * Untrained/accidental insiders: False sense of security, weak awareness regarding patching necessity and weak threat intelligence process | | |
| **Threat Event** | The event may occur in a single event and can also occur through a series of decision-making processes, which occur inside the I&T projects and within the relevant business department. | | |
| **Assets/Resources** | All I&T systems | | |
| **Consequence** | Increased exposure to risk due to poor coverage and implementation of patching processes | | |
| **Impact Dimensions (potential forms of loss)** | * Productivity | Productivity losses because a successful vulnerability exploitation may lead to services disruption |
| * Cost of Response | Response costs are payroll costs for incident responders, communications, PR, management meetings, forensics, etc., during an incident due to the exploited vulnerability. |
| * Replacement Cost | If the vulnerability exploitation causes severe damage to the system, replacement costs may be needed. |
| * Competitive Advantage | Competitive advantage may be impacted by significant productivity loss and reputation harm. |
| * Reputation | If the incident affects a customer-facing service for a significant time period, the organization reputation is negatively impacted. |
| * Fines and Judgements | N/A |
| **Timing** | Incident can be severe if it takes place during a mission-critical business period. | | |

|  |  |  |
| --- | --- | --- |
| 1. **Risk Scenario Scope & Extent** | | |
| **Extent of the Scenario** | **Worst Case** | Vulnerability of a customer-facing server is exploited, resulting in:   1. Website deface and service unavailability 2. Lateral movement into organization internal network successfully obtains Super User privileges (e.g., domain administrator account) 3. Leaked organization data, including confidential and personal data |
| **Typical or Most Likely Case** | Vulnerability exploitation results in service unavailability or website deface. Recovery procedures are in place and restoration is possible. Cost of clean-up and productivity losses occur due to website availability. |
| **Best Case** | Vulnerability exploitation results in providing read-only access to the attacker in a website folder tree that does not include confidential or personal data. |
| **Assumptions** | * Patch management process is ad-hoc and unevenly applied across I&T assets. * Organization is required to have PCI compliance but does not implement compliance across the whole of the I&T infrastructure. | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 1. **Controls to Mitigate the Risk Scenario** | | | | | | |
| **Control Description** | | **Control Type** | **Effect on Impact** | **Effect on Frequency** | **Essential Control** | **Reference** |
| 1 | **EDM05.02 Direct stakeholder engagement, communication and reporting.**  Ensure the establishment of effective stakeholder involvement, communication and reporting, including mechanisms for ensuring the quality and completeness of information, overseeing mandatory reporting and creating a communication strategy for stakeholders. | Preventive | Yes | No | Yes | COBIT EDM05.02 |
| 2 | **APO01.02 Communicate management objectives, direction and decisions made.**  Communicate awareness and promote understanding of alignment and I&T objectives to stakeholders throughout the enterprise. Communicate at regular intervals on important I&T-related decisions and their impact for the organization. | Preventive | Yes | Yes | yes | COBIT APO01.02 |
| 3 | **APO01.09 Define and communicate policies and procedures.**  Put in place procedures to maintain compliance with and performance measurement of policies and other components of the control framework. Enforce the consequences of noncompliance or inadequate performance. Track trends and performance and consider these in the future design and improvement of the control framework. | Preventive | Yes | Yes | Yes | COBIT APO01.09 |
| 4 | **APO11.03 Manage quality standards, practices and procedures and integrate quality management into key processes and solutions.**  Identify and maintain standards, procedures and practices for key processes to guide the enterprise in meeting the intent of the agreed quality management standards (QMS). This activity should align with I&T control framework requirements. Consider certification for key processes, organizational units, products or services | Preventive | Yes | Yes | Yes | COBIT APO11.03 |
| 5 | **DSS05.02 Manage network and connectivity security.**  Use security measures and related management procedures to protect information over all methods of connectivity. | Preventive | Yes | Yes | Yes | COBIT DSS05.02 |
| 6 | **DSS05.07 Manage vulnerabilities and monitor the infrastructure for security-related events.**  Using a portfolio of tools and technologies (e.g., intrusion detection tools), manage vulnerabilities and monitor the infrastructure for unauthorized access. Ensure that security tools, technologies and detection are integrated with general event monitoring and incident management. | Detective | Yes | Yes | Yes | COBIT DSS05.07 |

|  |  |  |  |
| --- | --- | --- | --- |
| 1. **Key Risk Indicators** | | | |
|  | **Indicator** | **KRI Description** | **Lead/Lag** |
| 1 | Organizational communications | Number of breaches of mandatory reporting requirements | Lag |
| 2 | Organizational communications | Frequency of communication on management objectives and direction for I&T | Lead |
| 3 | Vulnerability management | Number of vulnerabilities discovered | Lead |
| 4 | Vulnerability management | Percentage of systems that are covered by the threat intelligence process | Lead |
| 5 | Vulnerability management | Number of vulnerability tests carried out on perimeter devices | Lag |
| 6 | Vulnerability management | Number of vulnerabilities discovered during testing | Lead |
| 7 | Vulnerability management | Time taken to remediate any vulnerabilities | Lag |
| 8 | Incident response | Percent of time network and systems not available due to security incident | Lag |
| 9 | Incident response | Percent of tickets created in a timely manner when monitoring systems to identify potential security incidents | Lead |