| **IT Risk Scenario: Phishing Attack** | | | |
| --- | --- | --- | --- |
| 1. **Risk Scenario Description** | | | |
| **Risk Scenario Title** | Enterprise data are stolen through unauthorized access gained by a phishing attack | | |
| **Risk Type** | 3-Data and system protection | | |
| **Risk Scenario Category** | Internal and external security threats (e.g., hacker, malware): Malicious access to and compromise or misuse of technology systems, impacting the confidentiality, integrity or availability of technology systems and business information | | |
| **Risk Scenario Reference** | 10H | | |
| **Risk Statement** | A malicious actor launches a cyberattack via phishing emails, affecting the confidentiality, integrity and availability of assets. | | |
| **Risk Owner** | Business process owner | **Risk Oversight** | CISO |

|  |  |  |  |
| --- | --- | --- | --- |
| 1. **Risk Scenario Components** | | | |
| **Actor/Threat Community** | Cybercriminals, hacktivists, untrained/accidental insiders, malicious insiders and malicious accidental insiders | | |
| **Intent/ Motivation** | Phishing attacks are generally launched by external malicious actors with the intention of financial gain, causing reputational harm, or committing cyber espionage. They are typically enabled by accidental actions by untrained internal employees. | | |
| **Threat Event** | Possible threat events mainly include the exploitation of human factor with the use of social engineering methods combined with distribution of malicious software. | | |
| **Assets/Resources** | * Any organization system or asset * Any data stored on affected systems * System availability | | |
| **Consequence** | Response costs and reputation issues while under certain circumstances; significant costs may include productivity, competitive advantage loss and regulatory fines. | | |
| **Impact Dimensions (potential forms of loss)** | * Productivity | Productivity losses are relevant in cases where the organization did not maintain backup files of the stolen data and, hence, data are not available and need to be re-created. |
| * Cost of Response | Response costs are present, as incident responders, communications, PR, management meetings, forensics, etc. and work on the incident depending on severity. |
| * Replacement Cost | Usually there is no need for capital assets replacement on this scenario |
| * Competitive Advantage | Competitive advantage should be seriously considered because data lost may include confidential enterprise information (e.g., innovative ideas, strategic plans, source code, intellectual property). |
| * Reputation | If the incident affects customers and is severe enough, reputation may be impacted. |
| * Fines and Judgements | If enterprise data include personal data, then regulatory fines may be imposed (e.g., GDPR, CCPA, FTC). |
| **Timing** | * The **duration** of the incident can be very short or prolonged. * Early **detection** of the data loss is key to minimizing the impact. | | |

|  |  |  |
| --- | --- | --- |
| 1. **Risk Scenario Scope & Extent** | | |
| **Extent of the Scenario** | **Worst Case** | The attacker resides within the enterprise network for months, and data are leaked gradually to avoid detection. A worst-case scenario includes confidential enterprise data and customers’ personal and sensitive data. |
| **Typical or Most Likely Case** | The attacker obtains confidential information that does not include detailed intellectual property information or a subset of customers’ personal data. |
| **Best Case** | A compromised user account or workstation infection is detected and contained. Bits of enterprise information may be leaked but with no value for the adversary. |
| **Assumptions** | * The organization has systems or data critical to business processes. * The organization uses email to communicate. | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 1. **Controls to Mitigate the Risk Scenario** | | | | | | |
| **Control Description** | | **Control Type** | **Effect on Impact** | **Effect on Frequency** | **Essential Control** | **Reference** |
| 1 | **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 |
| 2 | **APO12.02 Analyze risk.**  Periodical risk assessment and risk management in general are essential to identify potential risk, its impact and probability, including for this risk scenario. This control is at the core of other more specific controls and needed to identify them properly. | Preventive | Yes | Yes | Yes | COBIT APO12.02 |
| 3 | **DSS01.03 Monitor I&T infrastructure.**  The proper continuous monitoring of the I&T infrastructure ensures that lack of compliance with controls or new types of events (e.g. potential malware, new vulnerabilities) are identified swiftly. | Preventive | Yes | Yes | Yes | COBIT DSS01.03 |
| 4 | **DSS05.03 Manage endpoint security.**  Ensure that endpoints (e.g., laptop, desktop, server, and other mobile and network devices or software) are secured at a level that is equal to or greater than the defined security requirements for the information processed, stored or transmitted. | Preventive | Yes | Yes | Yes | COBIT DSS05.03 |
| 5 | **DSS05.04 Manage user identity and logical access.**  Ensure that all users have information access rights in accordance with business requirements. Coordinate with business units that manage their own access rights within business processes. | Preventive | Yes | Yes | Yes | COBIT DSS05.04 |
| 6 | **DSS06.03 Manage roles, responsibilities, access privileges and levels of authority.**  Manage business roles, responsibilities, levels of authority and segregation of duties needed to support the business process objectives. Authorize access to all information assets related to business information processes, including those under the custody of the business, IT and third parties. This ensures that the business knows where the data are and who is handling data on its behalf. | Preventive | Yes | Yes | Yes | COBIT DSS06.03 |
| 7 | **DSS04.01 Define the business continuity policy, objectives and scope.**  Define business continuity policy and scope, aligned with enterprise and stakeholder objectives, to improve business resilience | Preventive | Yes | Yes | Yes | COBIT DSS04.01 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 8 | **DSS04.02 Maintain business resilience.**  Evaluate business resilience options and choose a cost-effective and viable strategy that will ensure enterprise continuity, disaster recovery and incident response in the face of a disaster or other major incident or disruption. | Preventive | Yes | Yes | Yes | COBIT DSS04.02 |

|  |  |  |  |
| --- | --- | --- | --- |
| 1. **Key Risk Indicators** | | | |
|  | **Indicator** | **KRI Description** | **Lead/Lag** |
| 1 | Organizational communications | Frequency of communication on management objectives and direction for I&T | Lead |
| 2 | Organizational communications | Percentage of customer requirements and expectations communicated throughout the business and IT organization | Lead |
| 3 | Training & awareness | Percentage of individuals receiving awareness training relating to use of endpoint devices | Lead |
| 4 | Training & awareness | Percentage of staff aware and able to demonstrate competency with respect to policies and procedures | Lead |
| 5 | Asset management | Number of accounts (vs. number of authorized users/staff) | Lead |
| 6 | Risk management | Percentage of successful security risk scenario simulations | Lead |
| 7 | Risk management | Percentage of key business processes included in the risk profile | Lead |
| 8 | Risk management | Percentage of key stakeholders involved in business impact analyses evaluating the impact over time of a disruption to critical business functions and the effect that a disruption would have on them | Lead |
| 9 | Business continuity planning | Percentage of key stakeholders participating, defining and agreeing on continuity policy and scope | Lead |
| 10 | Access management | Percentage of business process roles with assigned access rights and levels of authority | Lead |