Cyber Risk Checklist Across Project Phases Generated by Fine-Tuned GPT-4o-Mini

|  |  |  |
| --- | --- | --- |
| Phase | Different terms | Cyber risks |
| Initiation | pre-planning, concept, feasibility study, conception, early project definition, inception | 1. Weak Identity and Access Management. Inadequate access controls, such as the absence of multi-factor authentication, can allow unauthorized individuals to access sensitive project systems and data. 2. Unauthorized Access to Project Documents. Without proper safeguards, critical bidding documents and project plans may be viewed, stolen, or altered by unauthorized personnel. 3. Insecure Communication Channels. Using unencrypted emails or unsecured messaging platforms can lead to the interception of sensitive project information during transmission. 4. Inadequate Data Encryption. Failing to encrypt data both at rest and in transit makes sensitive project information vulnerable to breaches and unauthorized access. 5. Phishing Attacks Targeting Key Personnel. Deceptive emails or websites can trick project managers and team members into revealing login credentials or confidential project details. 6. Third-Party Vendor and Supply Chain Risks. Cyber vulnerabilities from subcontractors or technology providers with weak security measures can indirectly compromise the main project’s security. 7. Ransomware Attacks on Bidding Systems. Ransomware can lock access to essential project documents and systems, causing significant delays and disruptions during project initiation. 8. Lack of Cybersecurity Governance. The absence of formal cybersecurity policies and procedures can result in inconsistent security practices and leave the project exposed to various cyber threats. 9. Insider Threats. Employees, contractors, or other insiders with access to project systems and sensitive information may intentionally or unintentionally compromise security, leading to data breaches or system disruptions. 10. Inadequate Incident Response Planning. Without a well-defined incident response plan, the project team may struggle to effectively address and mitigate cybersecurity incidents, resulting in prolonged downtime and increased costs. |
| Design | design development, schematic design, detailed design, planning | 1. Unauthorized Access to Design and Construction Information. Unauthorized individuals or third parties gain access to confidential, proprietary, or sensitive project data. 2. Use of Outdated or Unsupported Design Tools (e.g., BIM). Utilizing outdated software versions increases susceptibility to security vulnerabilities and cyber attacks. 3. Failure to Apply Software Patches and Updates. Neglecting to update software can leave systems exposed to known vulnerabilities that attackers can exploit. 4. Exploitation of System Vulnerabilities. Cybercriminals exploit weaknesses in software or systems to access, modify, or erase critical project data. 5. Insufficient Data Sharing Regulations and Security Controls. Lack of robust policies and security measures in data sharing processes can lead to data leaks and unauthorized disclosures. 6. Insider Threats. Employees or contractors with legitimate access may intentionally or unintentionally compromise data security. 7. Phishing and Social Engineering Attacks. Attempts to deceive project stakeholders into divulging sensitive information or credentials, facilitating unauthorized access. 8. Ransomware and Malware Attacks. Malicious software disrupts design workflows, encrypts critical data, and demands ransom for restoration. 9. Intellectual Property Theft. Cyber espionage aimed at stealing proprietary designs, plans, and innovations to benefit competitors or malicious entities. 10. Data Breaches via Insecure Cloud Storage or Third-Party Services. Inadequate security measures in cloud platforms or third-party integrations can result in unauthorized access to project data. |
| Construction &Procurement | construction, procurement, build, execution, implementation | 1. Unauthorized Access to Design and Construction Information. Unauthorized individuals or entities gain access to sensitive project data, compromising confidentiality and integrity. 2. Exploitation of IoT Devices for Data Theft and Operational Disruption. Cyber attackers target Internet of Things (IoT) devices to steal data, disrupt operations, or manipulate processes, affecting the project’s functionality and security. 3. Supply Chain Cyber Attacks. Cyber threats targeting suppliers and subcontractors introduce vulnerabilities into the main project, potentially leading to data breaches or operational disruptions. 4. Ransomware Attacks on Procurement Systems. Malicious software encrypts procurement data, rendering systems unusable until a ransom is paid, causing significant project delays and financial losses. 5. Phishing and Social Engineering Targeting Procurement Personnel. Attempts to deceive procurement staff into revealing sensitive information or credentials, facilitating unauthorized access to procurement systems and data. 6. Vulnerabilities in Procurement Software and Platforms. Weaknesses in procurement software can be exploited by cybercriminals to gain unauthorized access, manipulate data, or disrupt procurement activities. 7. Manipulation of Bidding and Tender Processes. Cyber attackers may interfere with the bidding process by altering, deleting, or tampering with bids and tender documents, leading to unfair contractor selection and project delays. 8. Compromised Supplier Credentials. If supplier or procurement personnel credentials are compromised, attackers can access procurement systems, manipulate orders, or steal sensitive procurement data. |
| Commissioning | handover, startup, completion, closeout | 1. Unauthorized Access to Commissioning Data and System. Unauthorized individuals or entities gain access to sensitive commissioning data and control systems, compromising confidentiality and operational integrity. 2. Infiltration of Malware into Commissioning Systems. Cyber attackers introduce malicious software into commissioning systems, which can disrupt operations, corrupt data, or provide a gateway for further cyber intrusions. 3. Social Engineering Attacks Targeting Commissioning Personnel. Attempts to deceive commissioning staff into revealing sensitive information or credentials, facilitating unauthorized access to commissioning systems and data. 4. Insufficient Cybersecurity Measures for IoT Devices in Commissioning. Weak security protocols for Internet of Things (IoT) devices used during commissioning can lead to data breaches, unauthorized access, or manipulation of device functions. 5. Vulnerable Communication Channels Between Commissioning Teams and Systems. Insecure communication protocols can allow interception or manipulation of data transmitted between commissioning teams and control systems, leading to data breaches or operational disruptions. 6. Weak Access Controls and Identity Verification Mechanisms. Limited or ineffective access controls and identity verification processes can enable unauthorized personnel to access commissioning systems and data, increasing the risk of insider threats and external breaches. 7. Denial of Service (DoS) Attacks on Commissioning Systems. Cyber attackers may overwhelm commissioning systems with excessive traffic or requests, rendering them unavailable to legitimate users and causing significant delays in commissioning activities. 8. Inadequate Patch Management for Commissioning Software. Failure to regularly update and patch commissioning software can leave systems vulnerable to known exploits, allowing unauthorized access, disruptions, or data theft. 9. Unsecured Remote Access to Commissioning Systems. Providing remote access without robust security measures can expose commissioning systems to unauthorized access, data breaches, and potential manipulation of commissioning processes. |
| Operation & Maintenance | operation, maintenance, operations phase, facility management, service phase | 1. Unauthorized Access to Design and Construction Data. Unauthorized individuals or entities gain access to sensitive design and construction data, compromising confidentiality and integrity. 2. Leakage or Interference with Critical Asset Information. Sensitive information related to critical assets is leaked or tampered with, potentially disrupting operations and undermining asset security. 3. Manipulation of Construction Models and Maintenance Plans. Cyber attackers alter construction models or maintenance plans, leading to flawed operations, increased downtime, or inefficient maintenance activities. 4. Malicious Software Threats (e.g., Keystroke Loggers, Logic Bombs). Deployment of malicious software such as keystroke loggers, logic bombs, or unauthorized file downloads can disrupt systems, steal data, or cause operational failures. 5. Attacks Leading to Physical Damage and Theft of Intellectual Property. Cyber attacks targeting operational systems can result in physical damage to assets, theft of intellectual property, and harm to third-party assets. 6. Insufficient Protection of Third-Party Assets and Integrations. Weak security measures for third-party integrations and assets can create vulnerabilities, allowing attackers to exploit interconnected systems. 7. Unauthorized Remote Access to Operational Systems. Cyber attackers may exploit unsecured networks or weak authentication methods to gain remote access to operational systems, leading to manipulation, data breaches, or operational disruptions. 8. Insider Threats Compromising Operational Security. Employees, contractors, or other insiders with legitimate access may intentionally or unintentionally compromise security through misuse of credentials, data mishandling, or introducing vulnerabilities. 9. Inadequate Backup and Disaster Recovery Processes. Failure to implement robust backup and disaster recovery plans can result in data loss and prolonged downtime during cyber incidents or system failures, affecting maintenance activities and overall operations. 10. Vulnerabilities in Legacy Systems and Equipment. Older systems and equipment may lack modern security features, making them susceptible to cyberattacks. Exploiting these vulnerabilities can lead to unauthorized access, data breaches, and operational disruptions. |
| Renovation & End of Life | renovation, end of life, demolition, decommissioning, retrofitting, rehabilitation, disposal | 1. Unauthorized Access to Demolition Plans and Schedule. Unauthorized individuals or entities gain access to sensitive demolition plans and schedules, compromising project confidentiality and enabling potential sabotage or data manipulation. 2. Disclosure or Theft of Sensitive Demolition-Related Information. Sensitive information related to demolition activities, including proprietary methods, safety protocols, and project timelines, is leaked or stolen, leading to competitive disadvantages or security vulnerabilities. 3. Inadequate Identity and Access Management for Demolition Systems. Weak or improperly managed identity and access controls for demolition-related systems allow unauthorized personnel to access, modify, or disrupt critical operations and safety controls. 4. Insecure Communication and Data Transmission Among Stakeholders. Lack of secure communication protocols and encryption during data transmission among stakeholders can lead to interception, data breaches, and unauthorized access to sensitive information. 5. Social Engineering Attacks Targeting Demolition Personnel. Cyber attackers use deceptive tactics to manipulate demolition staff into divulging sensitive information or granting access to restricted systems, facilitating unauthorized access and potential sabotage. 6. Interference with Demolition Systems and Safety Controls. Cyber attackers disrupt demolition-related systems and safety controls through malware, unauthorized access, or system manipulation, potentially causing operational failures, safety hazards, and financial losses. 7. Unpatched or Outdated Software Utilized in the Demolition Process. Using outdated or unpatched software in demolition systems increases susceptibility to known vulnerabilities, allowing cybercriminals to exploit weaknesses and compromise system integrity. 8. Insider Threats Within Demolition Teams. Employees or contractors with legitimate access to demolition systems may intentionally or unintentionally compromise data security, leading to data leaks or system disruptions. 9. Insufficient Monitoring and Logging of Demolition Systems. Lack of comprehensive monitoring and logging mechanisms makes it difficult to detect and respond to unauthorized activities or breaches within demolition systems promptly. 10. Vulnerabilities in Third-Party Tools and Integrations. Integration of third-party tools and services in the demolition process can introduce vulnerabilities if these external systems lack robust security measures, providing potential entry points for cyber attacks. |