# Table G.1 Sample Threat Checklist

|  |  |
| --- | --- |
| **Threat** | **Applicable**  **Yes/No** |
| **Integrity** |
| Data stream could be intercepted. |  |
| Faulty programming could (inadvertently) modify data. |  |
| Copies of reports could be diverted (written or electronically) to unauthorized or unintended persons. |  |
| Data could be entered incorrectly. |  |
| Intentional incorrect data entry. |  |
| Use of outdated programs could compromise integrity of information. |  |
| Faulty hardware could result in inaccurate data entry and analysis. |  |
| Third parties could modify data. |  |
| Files could be accidentally deleted. |  |
| Hackers could change data. |  |
| Internal Users could launch unauthorized programs to access and or modify bank data. |  |
| Reports could be falsified |  |
| Internal theft of information by employees could be modified and used later. |  |
| Network sniffing could intercept user passwords and allow unauthorized modification of information |  |
| Information could be outdated. |  |
| Hackers could obtain unauthorized access into network to corrupt system resources. |  |
| Physical intrusion by unauthorized persons. |  |
| Documents could be falsified to appear as official company documents. |  |
| Unauthorized or fictitious sales could be approved. |  |
| Information could be misinterpreted due to language barriers. |  |
| Fraudulent programming could impact data integrity, example: hidden hooks. |  |
| Computer viruses could modify data. |  |
| Information could be misdirected. |  |
| Transactions could be intentionally not run or misrouted. |  |
| Newer or upgraded software could cause corruption of documents or files. |  |
| Non-standard procedures could cause misinterpretation of information. |  |
| Unauthorized persons may use an unattended workstation. |  |
| Information to and from 3rd parties could be corrupted in transmission. |  |
| Account Information may be shared. |  |
| A power failure could corrupt information. |  |
| Information could be submitted in a vague or misleading manner. |  |
| Someone could impersonate a customer to corrupt records (identity theft). |  |
| Information could be taken outside the company |  |
| Integrity of information could be compromised due to decay of information media. |  |
| Someone could impersonate an employee to corrupt information. |  |
| A terminated employee could intentionally corrupt information. |  |
| Company could be targeted for system hacking by a dissatisfied customer. |  |
| A default username and password for a network device could be exploited to gain access to system resources. |  |
| **Threat** | Applicable  Yes/No |
| **Confidentiality** |
| Insecure e-mail could contain confidential information. |  |
| Internal theft of information. |  |
| Employee is not able to verify the identity of a client, example: phone masquerading. |  |
| Confidential information is left in plain view on a desk. |  |
| Social discussions outside the office could result in disclosure of sensitive information. |  |
| Information could be salvaged by unauthorized persons from dumpsters or other waste receptacles. |  |
| Information sent to 3rd parties may be misused. |  |
| Unattended computer could give unauthorized access to files. |  |
| Passwords may not be required for all workstations. |  |
| Mailing two or more different customer statements/documents in one envelope. |  |
| Unauthorized people in confidential or restricted areas. |  |
| Confidential information may be left on the FAX or copy machine granting unauthorized viewing of documents. |  |
| Fraudulent or misrepresentation of individuals in phone conversations. |  |
| Response to a FAX request without verification. |  |
| Documents sent out for authorization could be forged and then returned. |  |
| Unauthorized access to information by viewing documents over the shoulder of an employee (shoulder surfing). |  |
| Documents could be excessively duplicated. |  |
| Employee passwords could be shared. |  |
| Inter office messengers may handle confidential information. |  |
| Employee and messenger relationships could exchange sensitive or confidential information. |  |
| Unauthorized disclosure of information by 3rd parties. |  |
| Not adequately destroying electronic media may leave information available to unauthorized persons. |  |
| Inadequate firewall configuration could inadvertently allow disclosure of information. |  |
| Actual client information could be used on templates causing disclosure of sensitive information. |  |
| Employees may be overheard discussing confidential information outside the office |  |
| Documents could be inadvertently delivered to wrong person. |  |
| Holding phone conversations when unable to verify identity. |  |
| Company could be subjected to electronic eavesdropping. |  |
| Terminated employees may be able to access the building or information. |  |
| Cleaning crews may see confidential information. |  |
| Rubbish could contain confidential information. |  |
| Employees may not follow the dual control procedures. |  |
| Temporary or new employees may be insufficiently trained. |  |
| Restricted areas may be accessed by visitors. |  |
| Use of the speaker phone may violate confidentiality. |  |
| Information and files may be inappropriately accessed on company’s systems. |  |
| Data stored off-site could be compromised. |  |
| Employee's may install illegal or unauthorized software. |  |
| Consultants or other contracted help may view confidential information. |  |
| **Threat** | **Applicable**  **Yes/No** |
| **Availability** |
| Files stored in personal directories may not be available to other employees when needed. |  |
| Hardware failures could impact the availability of company resources. |  |
| A failure in the data circuit could prohibit system access. |  |
| Act of God - Tsunami/hurricane |  |
| Upgrades in the software may prohibit access. |  |
| Company system could be unavailable or down. |  |
| Eating and drinking at a workstation could cause keyboard failure |  |
| An under-secured work area could jeopardize the confidentiality of customer information. |  |
| A power failure could interrupt employee access. |  |
| Software upgrades could affect other programs. |  |
| Expired user access and/or insufficient employee training could disrupt the computer system. |  |
| Availability of PC's shared by multiple users may be inadequate |  |
| Vendor or supplier support personnel may be unavailable due to the time zone differences. |  |
| A communication failure could disrupt business operations. |  |
| Employee's may have incorrect or inappropriate file access. |  |
| If a person is out (sick/absent) some critical files cannot be accessed. |  |
| Issues with 3rd party support to fix problems would give access to confidential information |  |
| An absent person or tools could prevent backup if not available. |  |
| Company could be subject to bombs or other acts of terrorism. |  |
| Theft of equipment or other information. |  |
| Insufficient cross-training of critical procedures could impact Fred's business processes. |  |
| Availability of information resources controlled by 3rd party could impact business processes. |  |
| Damaged or altered storage or hardware media. |  |
| Not all workstations have all programs loaded. |  |
| Users could lose or misplace files. |  |
| In today's environment there is a risk of man-made threats. |  |
| Geography and getting materials in, due to distance. |  |
| Vandalism and sabotage could be attempted to the network. |  |
| Number of software licenses could be Insufficient. |  |
| Insufficient personnel resources could impact business processes |  |
| A computer virus could be introduced via e-mail or disk. |  |
| Denial of Service Attacks from malicious internet users outside of Fred's. |  |
| Employee causes a document to be temporarily inaccessible due to human error. |  |
| **Threat** | **Applicable**  **Yes / No** |
| **Natural Threat** |
| Electrical storm |  |
| Ice storm |  |
| Snowstorm/Blizzard |  |
| Major landslide |  |
| Mudslide |  |
| Tsunami |  |
| Tornado |  |
| Hurricane / Typhoon |  |
| High Winds (70+ mph) |  |
| Tropical storm |  |
| Tidal flooding |  |
| Seasonal flooding |  |
| Local flooding |  |
| Upstream dam / reservoir failure |  |
| Sandstorm |  |
| Volcanic activity |  |
| Earthquake (2 – 4 on Richter scale) |  |
| Earthquake (5 or more) |  |
| Epidemic |  |
| **Threat** | **Applicable**  **Yes / No** |
| **Human - Accidental** |  |
| Fire: Internal-major |  |
| Fire: Internal-Catastrophic |  |
| Fire: External |  |
| Accidental explosion – on site |  |
| Accidental explosion – off site |  |
| Aircraft crash |  |
| Train crash |  |
| Derailment |  |
| Auto/Truck crash at site |  |
| Fire: Internal-minor |  |
| Human error – maintenance |  |
| Human error – operational |  |
| Human error – Programming |  |
| Human error – users |  |
| Toxic contamination |  |
| Medical emergency |  |
| Loss of key staff |  |
| **Threat** | **Applicable**  **Yes / No** |
| **Human - Deliberate** |  |
| Sabotage/Terrorism: External - Physical |  |
| Sabotage/Terrorism: Internal - Physical |  |
| Terrorism: Biological |  |
| Terrorism: Chemical |  |
| Bombing |  |
| Bomb Threat |  |
| Arson |  |
| Hostage taking |  |
| Vandalism |  |
| Labor dispute/Strike |  |
| Riot/Civil disorder |  |
| Toxic contamination |  |
| **Threat** | **Applicable**  **Yes / No** |
| **Environmental** |  |
| Power flux |  |
| Power outage – internal |  |
| Power outage – external |  |
| Water leak/plumbing failure |  |
| HVAC failure |  |
| Temperature inadequacy |  |
| Telecommunications failure |  |
| Toxic contamination |  |