Threat Listing

The table below provides a list of potential threats to [BUSINESS] information and information systems. This list is not exclusive, but intended to provide relevant examples to consider when evaluating the quantified impact and likelihood of a weakness being exploited.

Threat-Source	Threat	Description	Consequences
Human intentional/Human Unintentional	Data modification/ destruction/ corruption	An improperly protected system (e.g., unpatched or unprotected from malware) may allow data to be changed or destroyed.	Operational failure of [BUSINESS] (loss of availability and integrity). Damaged /[BUSINESS] reputation
Human intentional/Human Unintentional	Damage/destruction of assets	Destruction of the physical structure and IT assets will adversely affect the availability of a system.	Without infrastructure out of which to operate and without working IT assets, the systems supporting [BUSINESS] will not be available.

Human intentional/Human Unintentional	Data Loss/Information Disclosure	An improperly protected system (e.g., unpatched or unprotected from malware) may allow for the intentional or inadvertent leakage of sensitive data.	Data loss may affect the ability of the [BUSINESS] to meet its mission, but also open the up to litigation or result in serious damage to the 's reputation, including a costly response to any data leakage.
Human intentional/Human Unintentional	Unauthorized access	Access to systems and information which a person does not need can lead to data leakage or to the compromise of a system.	Operational failure of [BUSINESS] (loss of availability and integrity) Damaged /[BUSINESS] reputation.
Human intentional/Human Unintentional	Unauthorized changes to systems	When changes are not tracked or authorized, system integrity and availability come into question.	Changes made to the system that are not tracked adversely affect the ability to recover from a disaster, rebuild a system, or recognize current vulnerabilities that may exist on a system due to its configuration.
Environmental/ Natural	Temperature/humidity control	Without adequate temperature or humidity control, IT systems may suffer adverse physical failures and affect availability.	If temperatures get too hot or too cold, equipment failures occur and systems will not be available.
Environmental/ Natural	Power Failure	Inadequate power will adversely affect the availability of a system.	Without adequate power and backup power, the systems supporting [BUSINESS] will not be available.
Environmental/ Natural	Fire	Destruction of the physical structure and IT assets will adversely affect the availability of a system.	Without infrastructure out of which to operate and without working IT assets, the systems supporting [BUSINESS] will not be available.
Environmental/ Natural	Water damage	Destruction of the physical structure and IT assets will adversely affect the availability of a system.	Without infrastructure out of which to operate and without working IT assets, the systems supporting [BUSINESS] will not be available.

Environmental/ Natural	Inability to recover from a disaster	Without proper planning, resource support, and recovery documentation, the [BUSINESS] will be unable to recover from an event or disaster.	The inability to recover from a disaster can result in damage to 's reputation and the [BUSINESS]'s ability to support its mission.
Legal	Policy breach	The lack of policy or a violation of existing policy may open [BUSINESS] up to other threats and vulnerabilities, such as data loss, unauthorized access, or other vulnerabilities.	The lack of policy or a violation of existing policy may open the [BUSINESS] up to litigation or result in serious damage to the 's reputation
Managerial	Lack of Resources	Resources, including personnel and life cycle replacement of IT components, if not adequately put in place, can cause system failures or inability to provide adequate support to the [BUSINESS] mission.	Without adequate resources, the [BUSINESS] has suffered single points of failure which caused repeated repair or reinvention of processes.
Managerial	Incomplete documentation	Without an accurate inventory of managed systems within the [BUSINESS] or maintenance information, security controls may not be effectively applied and subject the system to other vulnerabilities or exploits.	Undocumented systems may be used to exploit the [BUSINESS].