Threat Statement Table

ID	Threat Name	Type Identifier	Example	Description	Typical Impact to Data or System		
					Confidentiality	Integrity	Availability
T-1	Alteration	U, P, E		Alteration of data, files, or records.		Modification	
T-2	Audit Compromise	P		An unauthorized user gains access to the audit trail and could cause audit records to be deleted or modified, or prevents future audit records from being recorded, thus masking a security relevant event.		Modification or Destruction	Unavailable Accurate Records
T-3	Bomb	P		An intentional explosion.		Modification or Destruction	Denial of Service
T-4	Communications Failure	U, E	San Diego County, February 2019 https://www.nbcsandiego.com/news/local/storm-system-weather-damages-tree-poles-fall-power-outages-rain-wind/6013/ See Appendix for more details	Cut of fiber optic lines, trees falling on telephone lines.			Denial of Service
T-5	Compromising Emanations	P		Eavesdropping can occur via electronic media directed against large scale electronic facilities that do not process classified National Security Information.	Disclosure		

ID	Threat Name	Type Identifier	Example	Description	Typical Impact to Data or System		
					Confidentiality	Integrity	Availability
T-6	Cyber Brute Force	P	Alibaba's Taobao shopping site – 2016 https://www.reuters.com/article/us-alibaba-cyber/hackers-attack-20-million-accounts-on-alibabas-taobao-shopping-site-idUSKCN0VD14X See Appendix for more details	Unauthorized user could gain access to the information systems by random or systematic guessing of passwords, possibly supported by password cracking utilities.	Disclosure	Modification or Destruction	Denial of Service
T-7	Data Disclosure Attack	P		An attacker uses techniques that could result in the disclosure of sensitive information by exploiting weaknesses in the design or configuration.	Disclosure		
T-8	Data Entry Error	U		Human inattention, lack of knowledge, and failure to cross-check system activities could contribute to errors becoming integrated and ingrained in automated systems.		Modification	
T-9	Denial of Service Attack	P		An adversary uses techniques to attack a single target rendering it unable to respond and could cause denial of service for users of the targeted information systems.			Denial of Service
T-1	Distributed Denial of Service Attack	P	DDoS of CNN, Yahoo, eBay, Amazon, ETrade and other by "Mafiaboy", 2000 https://www.theguardian.com/world/2000/apr/20/terrorism See Appendix for more details	An adversary uses multiple compromised information systems to attack a single target and could cause denial of service for users of the targeted information systems.			Denial of Service
T-1	Earthquake	E		Seismic activity can damage the information system or its facility. Please refer to the following document for earthquake probability maps http://pubs.usgs.gov/of/2008/1128/pdf/OF08-1128_v1.1.pdf .		Destruction	Denial of Service

ID	Threat Name	Type Identifier	Example	Description	Typical Impact to Data or System		
					Confidentiality	Integrity	Availability
T-1	Electromagnetic Interference	E, P		Disruption of electronic and wire transmissions could be caused by high frequency (HF), very high frequency (VHF), and ultra-high frequency (UHF) communications devices (jamming) or sun spots.			Denial of Service
T-1	Espionage	P		The illegal covert act of copying, reproducing, recording, photographing or intercepting to obtain sensitive information .	Disclosure	Modification	
T-1	Fire	E, P		Fire can be caused by arson, electrical problems, lightning, chemical agents, or other unrelated proximity fires.		Destruction	Denial of Service
T-1	Floods	E		Water damage caused by flood hazards can be caused by proximity to local flood plains. Flood maps and base flood elevation should be considered.		Destruction	Denial of Service
T-1	Fraud	P		Intentional deception regarding data or information about an information system could compromise the confidentiality, integrity, or availability of an information system.	Disclosure	Modification or Destruction	
T-1	Hardware or Equipment Failure	E		Hardware or equipment may fail due to a variety of reasons.			Denial of Service
T-1	Hardware Tampering	P		An unauthorized modification to hardware that alters the proper functioning of equipment in a manner that degrades the security functionality the asset provides.		Modification	Denial of Service
T-1	Hurricane	E		A category 1, 2, 3, 4, or 5 land falling hurricane could impact the facilities that house the information systems.		Destruction	Denial of Service

ID	Threat Name	Type Identifier	Example	Description	Typical Impact to Data or System		
					Confidentiality	Integrity	Availability
T-2	Malicious Software	P		Software that damages a system such a virus, Trojan, or worm.		Modification or Destruction	Denial of Service
T-2	Phishing Attack	P	Lancaster University, 2019 https://www.zdnet.com/article/phishing-attack-students-personal-information-stolen-in-university-data-breach/ See Appendix for more details	Adversary attempts to acquire sensitive information such as usernames, passwords, or SSNs, by pretending to be communications from a legitimate/trustworthy source. Typical attacks occur via email, instant messaging, or comparable means; commonly directing users to Web sites that appear to be legitimate sites, while actually stealing the entered information.	Disclosure	Modification or Destruction	Denial of Service
T-2	Power Interruptions	E		Power interruptions may be due to any number of reasons such as electrical grid failures, generator failures, uninterruptable power supply failures (e.g. spike, surge, brownout, or blackout).			Denial of Service
T-2	Procedural Error	U		An error in procedures could result in unintended consequences.	Disclosure	Modification or Destruction	Denial of Service
T-2	Procedural Violations	P		Violations of standard procedures.	Disclosure	Modification or Destruction	Denial of Service
T-2	Resource Exhaustion	U		An errant (buggy) process may create a situation that exhausts critical resources preventing access to services.			Denial of Service

ID	Threat Name	Type Identifier	Example	Description	Typical Impact to Data or System		
					Confidentiality	Integrity	Availability
T-2	Sabotage	P		Underhand interference with work.		Modification or Destruction	Denial of Service
T-2	Scavenging	P		Searching through disposal containers (e.g. dumpsters) to acquire unauthorized data.	Disclosure		
T-2	Severe Weather	E		Naturally occurring forces of nature could disrupt the operation of an information system by freezing, sleet, hail, heat, lightning, thunderstorms, tornados, or snowfall.		Destruction	Denial of Service
T-2	Social Engineering	P	"The Ark" Los Angeles 1979 https://www.mitnicksecurity.com/in-the-news/legendary-most-wanted-hacker-reveals-the-latest-cybercrime-schemes See Appendix for more details	An attacker manipulates people into performing actions or divulging confidential information, as well as possible access to computer systems or facilities.	Disclosure		
T-3	Software Tampering	P		Unauthorized modification of software (e.g. files, programs, database records) that alters the proper operational functions.		Modification or Destruction	
T-3	Terrorist	P		An individual performing a deliberate violent act could use a variety of agents to damage the information system, its facility, and/or its operations.		Modification or Destruction	Denial of Service
T-3	Theft	P		An adversary could steal elements of the hardware.			Denial of Service

ID	Threat Name	Type Identifier	Example	Description	Typical Impact to Data or System		
					Confidentiality	Integrity	Availability
T-3	Time and State	P		An attacker exploits weaknesses in timing or state of functions to perform actions that would otherwise be prevented (e.g. race conditions, manipulation user state).	Disclosure	Modification	Denial of Service
T-3	Transportation Accidents	E		Transportation accidents include train derailments, river barge accidents, trucking accidents, and airlines accidents. Local transportation accidents typically occur when airports, sea ports, railroad tracks, and major trucking routes occur in close proximity to systems facilities. Likelihood of HAZMAT cargo should be determined when considering the probability of local transportation accidents.		Destruction	Denial of Service
T-3	Unauthorized Facility Access	P		An unauthorized individual accesses a facility which may result in comprises of confidentiality, integrity, or availability.	Disclosure	Modification or Destruction	Denial of Service
T-3	Unauthorized Systems Access	P		An unauthorized user accesses a system or data.	Disclosure	Modification or Destruction	
T-3	Volcanic Activity	E		A crack, perforation, or vent in the earth's crust followed by molten lava, steam, gases, and ash forcefully ejected into the atmosphere. For a list of volcanoes in the U.S. please see http://volcanoes.usgs.gov/about/volcanoes/volcanolist.php .		Destruction	Denial of Service

Appendix

Examples:

- T4 – Communications failure – San Diego County February 2019 – Storm brings down the trees, utility poles, causes damage across county. Dozen of power outages throughout the county, affecting around 1,800 customers.

Johnson, A (2019, February 14). Storm Brings Down Trees, Utility Poles, Causes Damage Across County. Retrieved September 20, 2020 from https://www.nbcsandiego.com/news/local/storm-system-weather-damages-tree-poles-fall-power-outages-rain-wind/6013/

- T2 – Social Engineering – Kevin Mitnick used social engineering to access the developers account exposing weaknesses in humans.

Mitnick Security (2017, May 17). Legendary "most wanted" hacker reveals the latest cybercrime schemes. Retrieved September 20, 2020 from https://www.mitnicksecurity.com/in-the-news/legendary-most-wanted-hacker-reveals-the-latest-cybercrime-schemes

- T6 – Cyber Brute Force – Hackers obtained a database of 99 million usernames and passwords

Reuters Staff (2016, February 4). Hackers attack 20 million accounts on Alibaba's Taobao shopping site. Retrieved September 20,2020 from https://www.reuters.com/article/us-alibaba-cyber/hackers-attack-20-million-accounts-on-alibabas-taobao-shopping-site-idUSKCN0VD14X

- T1 - Distributed Denial of Service Attack – A 15-year old launched a successful DDoS attack against CNN, Yahoo, eBay, Amazon, ETrade and others. Three computers have been identified as middlemen in the February attacks: a computer at the University of California, Santa Barbara; a router at Stanford University; and a home business computer in the area of Portland, Oregon. Investigators say that dozens, even hundreds, of middlemen computers were used in the attacks.

The Guardian (2000, April 19) "Mafiaboy" charged with cyber-terrorism. Retrieved September 20, 2020 from https://www.theguardian.com/world/2000/apr/20/terrorism

- T2 – Phishing Attack – Hackers stolen personal data of Lancaster University students after gaining access to databases that contained personal information via a successful phishing attack delivered via email.

Palmer, D (2019, July 23) Phishing attack: Students' personal information stolen in university data breach. Retrieved September 20, 2020 from https://www.zdnet.com/article/phishing-attack-students-personal-information-stolen-in-university-data-breach/