Internal Threat Actors

Threat Actor Type	Motive	Modus Operandi (MO)	How Motive Drives MO
Malicious Insider	Financial gain	Data theft or exfiltration	Steals sensitive data (financial records, customer info, intellectual property) to sell on the dark web or for personal profit.
	Espionage	System manipulation, unauthorized access	Gains access to restricted systems or manipulates data for spying purposes, potentially working for a competitor or foreign government.
	Revenge	System sabotage, data destruction, AI-powered data manipulation	Sabotages systems, destroys data, or manipulates data using AI tools to cause harm to the organization out of anger or resentment.
Disgruntled Employee	Sabotage	Malware introduction, AI-powered sabotage	Introduces malware or uses AI tools to disrupt operations or cause damage to the organization's reputation, potentially for personal satisfaction or ideological reasons.
	Revenge	Data theft or destruction	Steals or destroys sensitive data to inflict damage on the organization out of spite or a desire for retaliation.
	Retribution	System sabotage	Sabotages systems or disrupts operations to get back at the organization for perceived injustices or mistreatment.
	Financial gain	Denial-of-service attacks	Launches DoS attacks to extort money from the organization or disrupt their operations, hoping to be paid to stop the attack.
		Spreading misinformation, AI-assisted disinformation campaigns	Spreads false or damaging information about the organisation,potentially using AI tools to amplify the reach or impact, to harm its reputation and potentially cause financial losses. This is motivated by bitterness or a desire to harm the organization.

External Threat Actors - 1/4

Threat Actor Type	Motive	Modus Operandi (MO)	How Motive Drives MO
Hacktivist	Ideological or political motives	Website defacement	Defaces websites with political messages or propaganda to raise awareness for their cause or to shame the target organization.
	Social change	Denial-of-service attacks	Disrupts online services with DoS attacks to bring attention to a social issue or protest against an organization's actions they deem harmful.
	Raising awareness	Data leaks	Leaks sensitive information to expose wrongdoing by an organization or to bring attention to an important social or environmental issue.
		AI-powered disinformation campaigns	Leverages AI to spread propaganda, create fake news, or manipulate public opinion to advance their political or social agenda.
Script Kiddie	Curiosity	Using readily available hacking tools	Experiments with hacking tools and techniques out of curiosity, often targeting easy-to-exploit vulnerabilities without a clear malicious goal.
	Bragging rights	Defacing websites	Defaces websites or leaves their mark to boast about their skills and gain recognition within the hacking community, seeking notoriety.
	Malicious intent (limited skills)	Launching basic DoS attacks, using basic AI-powered hacking tools	Launches basic DoS attacks to cause minor disruption, potentially using simple AI-powered tools for enhanced effectiveness. This is often done for amusement or to see if they can successfully disrupt a target.
		Spreading misinformation, AI-assisted disinformation campaigns	Spreads false or damaging information about the organization,potentially using AI tools to amplify the reach or impact, to harm its reputation and potentially cause financial losses. This is motivated by bitterness or a desire to harm the organization.

External Threat Actors - 2/4

Threat Actor Type	Motive	Modus Operandi (MO)	How Motive Drives MO
Organized Crime	Financial gain	Ransomware attacks, AI-powered ransomware	Encrypts data and demands ransom payments for decryption, potentially using AI to target high-value data or automate extortion processes, as it is a highly profitable and often successful method of extortion.
		Data theft and extortion	Steals valuable data (customer information, financial records) and threatens to expose or sell it unless a ransom is paid.
		Financial fraud	Uses stolen financial information (credit card numbers, bank accounts) to conduct fraudulent transactions, directly profiting from the stolen data.
		Phishing campaigns, AI-assisted phishing	Sends mass phishing emails, potentially using AI to personalize messages and increase effectiveness, to trick victims into revealing sensitive information, which is then used for financial gain through identity theft or account takeover.
	Money laundering	Money laundering through cryptocurrencies	Uses cryptocurrencies to launder illegally obtained funds, making it difficult for law enforcement to track and seize the proceeds of their crimes.

External Threat Actors - 3/4

Threat Actor Type	Motive	Modus Operandi (MO)	How Motive Drives MO
Nation-State	Espionage	Advanced Persistent Threats (APTs), AI-driven espionage	Uses sophisticated, long-term attacks, potentially enhanced by AI, to infiltrate government or corporate networks and steal sensitive data (military secrets, intellectual property) for strategic advantage.
	Sabotage	Data exfiltration	Extracts large amounts of data from critical infrastructure or government systems to disrupt operations, gain a strategic advantage, or weaken a target nation.
	Political influence	Disruption of critical infrastructure	Launches attacks against critical infrastructure (power grids, transportation, communication systems) to cause chaos, disrupt services, and undermine political stability in a target nation.
	Cyberwarfare	Spreading disinformation and propaganda, AI-assisted cyberwarfare	Uses social media and online platforms to spread propaganda, sow discord, and manipulate public opinion to influence elections or political movements in other nations, potentially using AI to enhance the reach and effectiveness of campaigns.

External Threat Actors - 4/4

Threat Actor Type	Motive	Modus Operandi (MO)	How Motive Drives MO
Competitor	Business advantage	Industrial espionage	Spies on rivals to steal trade secrets, intellectual property, or confidential business information to gain a competitive edge.
	Stealing intellectual property	Sabotage	Sabotages a competitor's systems or operations to disrupt their business, potentially gaining market share or damaging their reputation.
	Disrupting operations	Denial-of-service attacks	Launches DoS attacks against a competitor's websites or services to disrupt their operations, frustrating customers and potentially driving them away.
	Gaining market share	Data theft	Steals customer data or other sensitive information to gain a competitive advantage or damage a competitor's reputation, potentially luring customers away.
		Disinformation campaigns, AI-driven market manipulation	Spreads false or misleading information about a competitor or manipulates online markets using AI to damage their reputation and steer customers towards their own products or services, manipulating market perception.