SABOTAGE

TARGET + INTENT

Malicious insiders target physical, technical, or virtual assets and infrastructure with the intent to destroy, damage, disrupt, or compromise the functionality, confidentiality, integrity, or availability of an organization’s systems, data, operations, or premises.

AT RISK

1. Manufacturing processes or critical machinery
2. Critical servers or codes
3. Power grids and other critical infrastructures
4. Facilities, warehouses, and internal and external storage sites

FRAUD

TARGET + INTENT

Malicious insiders modify, add, or delete data or confidential information for their own personal gain or engage in fraud-related activities to facilitate external threat actors in carrying out deceptive criminal activity.

AT RISK

1. Personally identifiable Information (PII)
2. Proprietary or confidential customer lists
3. Information tied to insider trading, embezzlement, other actions to defraud an organization

VIOLENCE

TARGET + INTENT

Malicious insiders target people – typically motivated by someone or something related to an organization – with the intent to threaten or harm through acts that create an intimidating, hostile, abusive, or life-threatening environment and compromise the health and safety of employees, customers, visitors, and other bystanders.

AT RISK

1. Potential victims of criminal acts such as robbery
2. Potential victims of violent acts by customers or unknown others
3. Potential victims of violent acts carried out between co-workers
4. Potential direct and indirect victims of domestic violence that spills into the workplace
5. Potential victims of extreme acts of targeted violence or terrorism

ESPIONAGE

TARGET + INTENT

Malicious insiders target systems, networks, classified information, and national intelligence from a U.S. Government agency or organization for the benefit or a foreign nation, entity, or organization, or a new company the insider has established in a foreign country.

AT RISK

1. National intelligence
2. Proprietary software/source code
3. Business and strategic plans and proposals
4. Customer information
5. Product information (designs, formulas, schematics)

THEFT OF INTELLECTUAL PROPERTY

TARGET + INTENT

Malicious insiders target systems, data, or networks to steal intellectual property, proprietary products, trade secrets, or other intangible assets created and owned by an organization to gain a business advantage: either to take with them to a new job or to start their own competing business.

AT RISK

1. Proprietary software/source code
2. Business and strategic plans and proposals
3. Proprietary customer lists
4. Product information (designs, formulas, schematics)