Threat Modeling Use Case

Name: Multi-National Company

Category: Private Sector

Sponsoring Organization: Demandware, Inc./OMG

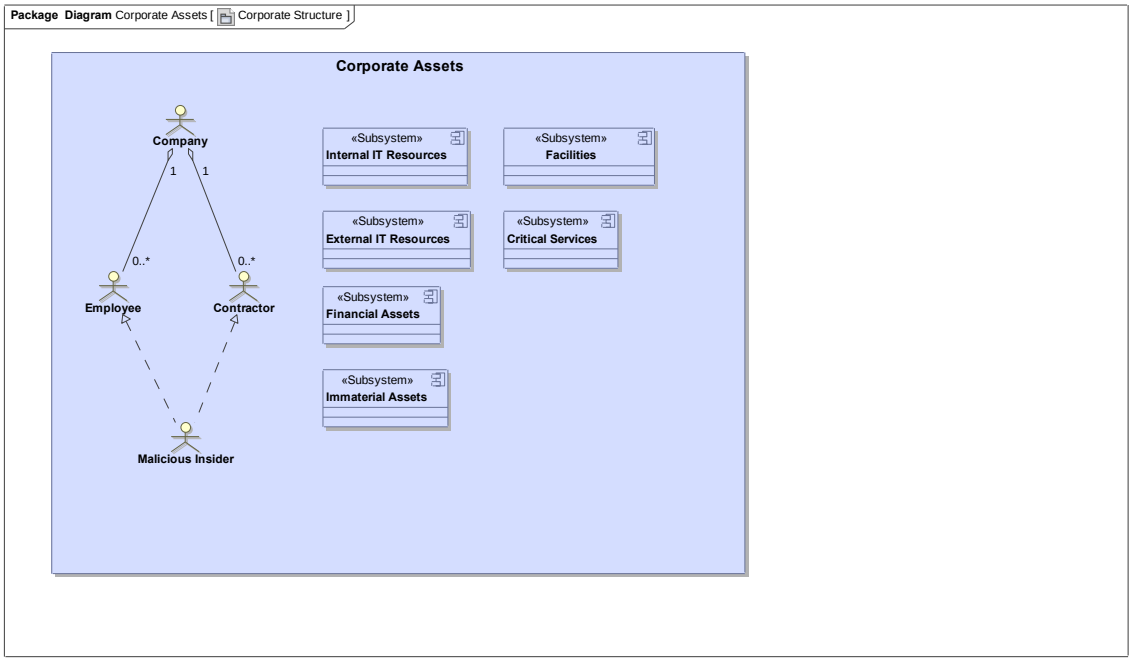
Affected Threat Domains
Cyber/Information Security
Facilities

1 Summary

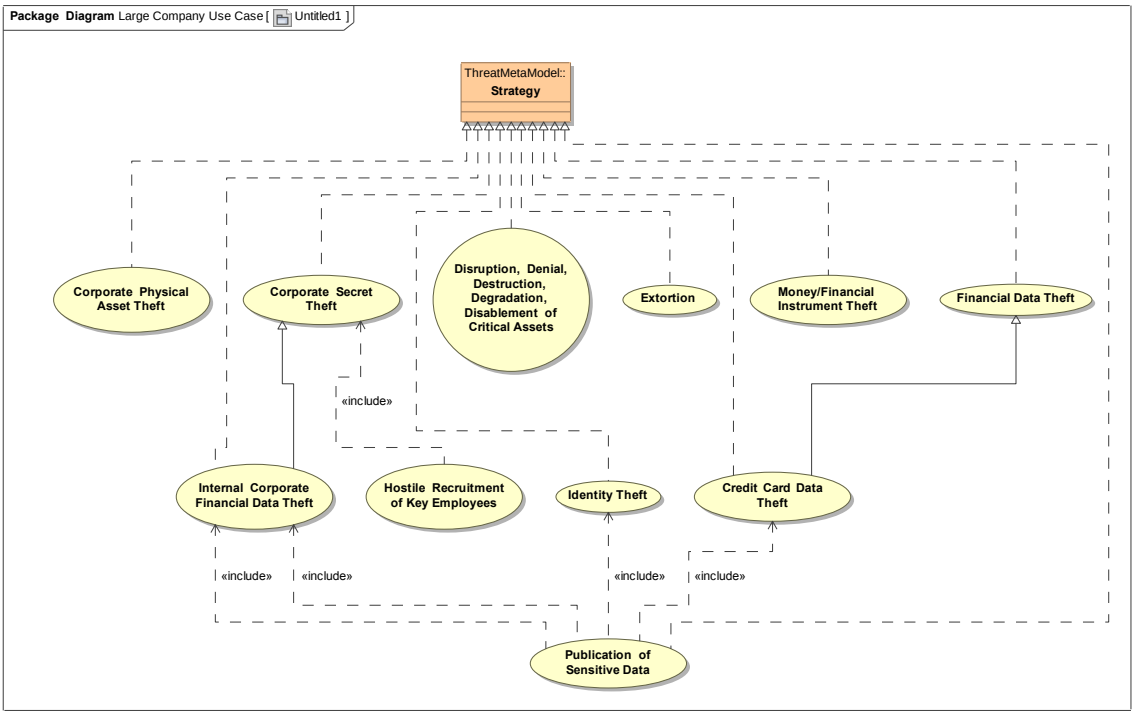
1.1 Description

- Multi-national company with multiple datacenters, office facilities, international business activity
  - Offices and data centers are located in the US, Europe, APAC
  - Some facilities are in the PR China, Hong Kong, Russia, and other problematic countries
  - Employees include US and foreign citizen, across all locations
  - Some data centers are hosted by a co-location provider with external security staff
  - Turn-over of staff is within normal ranges
  - Active use of contractors and other external partners
- Large number of deployed security systems, sensors
  - Information Security systems
    - Access control through directory, but large number of services that are not integrated
    - Basic endpoint security systems for most servers and laptops
    - Firewalls
    - IDS/IPS
    - SIEM
    - Systems monitoring
  - Physical Security systems
    - Basic physical access control
    - Video monitoring of sensitive areas
    - Intrusion detection
    - Commercial fire alarms and suppression
    - Notification/alerting for critical events (through SMS, email, etc.)
  - On call staff

- Skeletal 24/7 support team
- Some on-call staff for escalation
- External guards



A variety of potential attack scenarios can be played out against the company, including external and internal attacks. While there is a reasonable security program in place, the company is not able to ensure full in-depth security across all systems and assets for the following reasons. In these scenarios the following Strategies are employed:



Potential adversaries may include:

- Cyber criminals, including organized crime (domestic and foreign)
- Competitors
- Malicious Insiders: Disgruntled employees and contractors
- Hostile Investors: Potential corporate or individual acquirers of company
- Nation state adversaries (unlikely, unless company engages in critical infrastructure or national defense, etc.)
- Terrorist Organizations

2 Scenarios

2.1 Scenario: Financial Gain

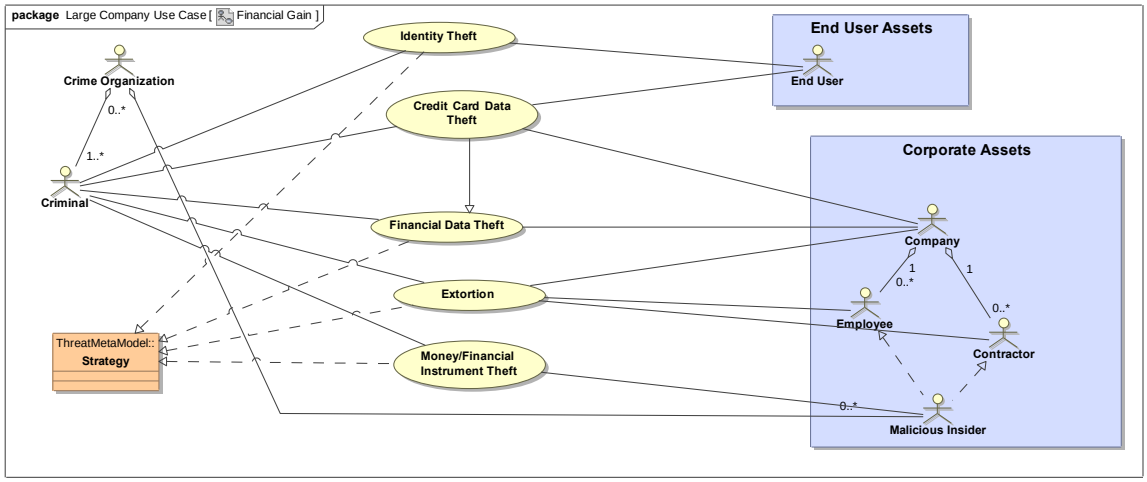
Main Actors:

- Cyber criminals/OC
- Malicious Insider

Main Strategies:

- credit card/sensitive financial data theft
- identity theft
- extortion
- Money/Financial Instrument Theft

Role of the Malicious Insider:
The Insider is simply an agent assisting the main actors in executing their attacks. The insider may be motivated by any reason.
For the case of money theft, the malicious insider can be a main actor.



2.1.1 Strategy: Identity Theft
The attacker attacks the end user systems or the corporate assets (cyber or traditional information assets) to obtain the identities of primarily the end users. Subsequently the attackers use these identities to create new credit accounts or access existing assets owned by the victims.

2.1.2 Strategy: Financial Data Theft
The attackers obtain sensitive financial information about end-users or other entities from corporate assets. These types of information may include credit card data. This information is used to extract money from the affected financial accounts.

2.1.3 Strategy: Extortion
The attacker obtains the ability to negatively affect corporate assets (e.g. through denial, destruction, disruption, degradation, distortion, data exfiltration, etc.) and blackmail the company. The company pays a ransom to avoid negative consequences.

2.1.4 Strategy: Money/Financial Instrument Theft
This is traditional direct theft of money (cash or cash-like instruments), or similar financial instruments that can immediately be sold. Both criminals as well as Insiders follow this strategy. This strategy may involve physical and/or cyber theft of money.

2.2 Scenario: Reputation Damage
Main Actors:
- Competitor
- Hostile Investor

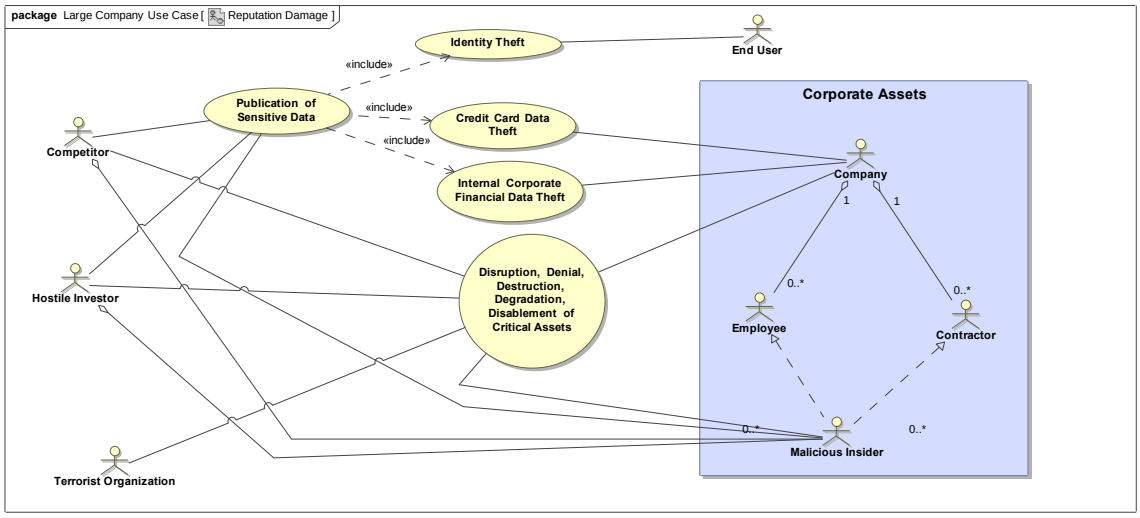
- Terrorist Organization
- Malicious Insider

Main Strategies:

- Theft Internal Financial Data
- Identity theft and publication
- Credit card/financial data theft and publication
- Disable, Destroy, Deny, Degrade, Disrupt Critical Assets

Role of the Malicious Insider:

In addition to assisting the other main actors for any reason, the malicious insider may also act as main actor. This may happen if the insider is estranged from the company and wishes to exact revenge for perceived or real injustice through the company.



2.2.1 Strategy: Identity Theft

The attacker steals personal identification belonging to the end-users of the company and publishes it subsequently. This is intended to embarrass the company and create doubt about their ability to protect data.

2.2.2 Strategy: Credit Card Data Theft

The attacker targets specifically credit card data and publish it subsequently. This is intended to specifically attack the company's credibility as a trustworthy merchant. It may result in additional fines, or even in loosing the ability to process credit cards in the future.

2.2.3 Strategy: Internal Corporate Financial Data Theft

By stealing and publishing the company's internal financial data, the attackers succeed in making internal sales and profit data public. Such data may be a surprise for markets and negatively affect investor sentiment. In addition it may result in regulatory actions against the company

2.2.4 Strategy: Disable, Destroy, Deny, Degrade, Disrupt Critical Assets

The attacker targets company critical assets and attempts to disable, destroy, deny, degrade, or disrupt (5-Ds) them. This may have a number of reasons:

- Disturb the use of critical assets and negatively influence the ability to operate, cause distraction with employees, customers, and partners
- Inflict damage on the company's ability to deliver core services specifically to customers (but also employees or partners)

2.3 Goal and Motivation: Stock Market Manipulation

Main Actors:

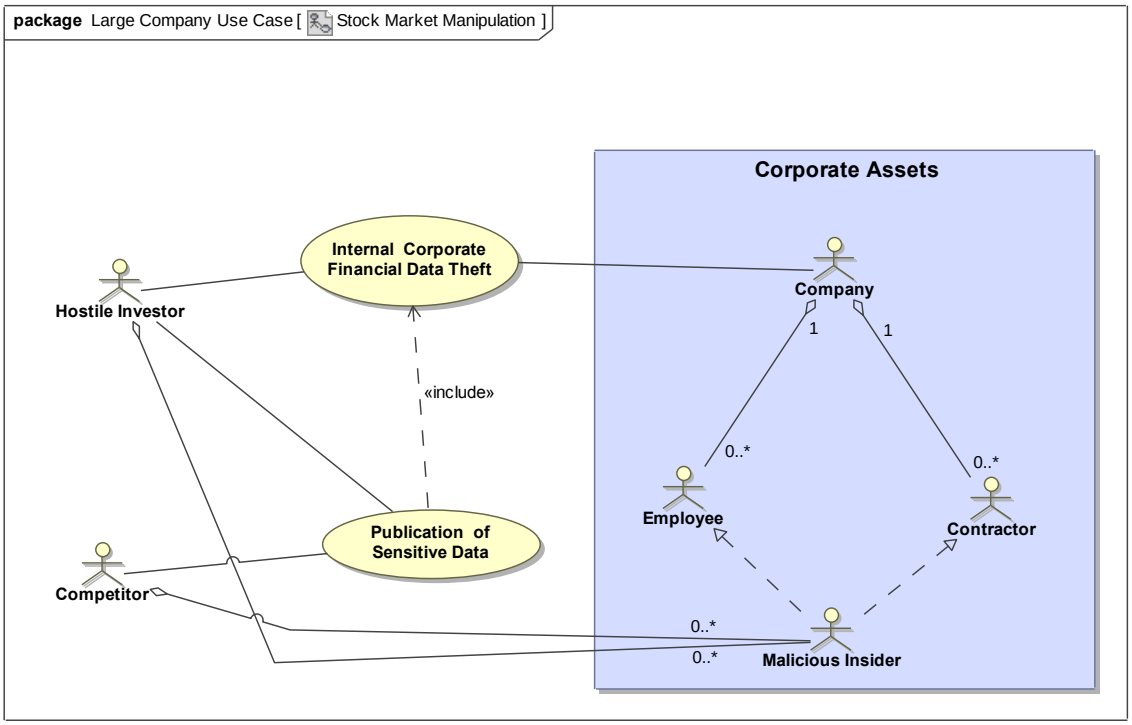
- Competitor
- Hostile Investor

Main Strategies:

- Publication of internal corporate financial data
- Theft of internal financial data

Role of the Malicious Insider:

The Insider is simply an agent assisting the main actors in executing their attacks. The insider may be motivated by any reason.



2.3.1 Strategy: Theft of Internal Corporate Financial Data

By stealing internal financial data, the hostile investor may gain additional insight into the company's financial situation. This can change their valuation of the

company and its associated risks, allowing them to enter stock transactions that would seem risky or irrational to outsiders.

2.3.2 Strategy: Publication of Internal Financial Data

Publication of internal financial data may expose internal deviations from market expectations (both positive and negative). If this happens at critical times, the stock price of the company may fluctuate significantly. This may result in special investment opportunities for the hostile investor, or create market benefits for competitors.

2.4 Scenario: Corporate Asset Theft

Main Actors:

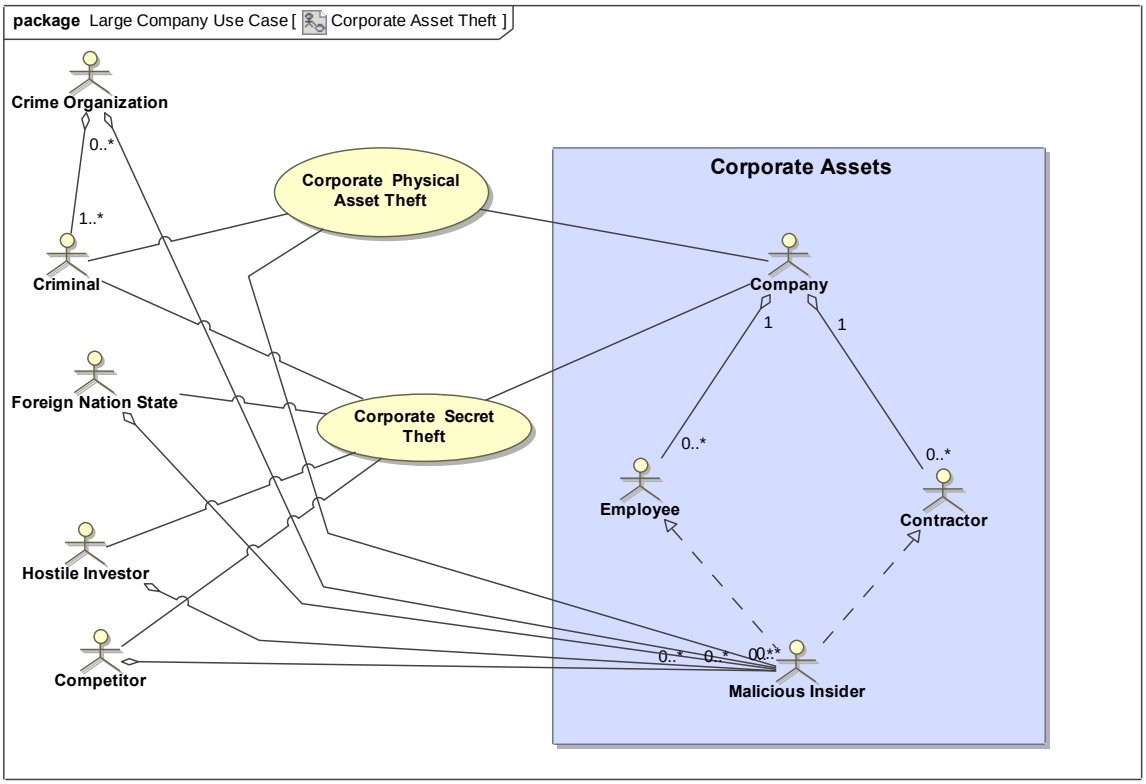
- Cyber criminals/OC
- Competitor
- Hostile Investor
- Foreign Nation State
- Malicious Insider

Main Strategies:

- Corporate secret theft (Corporate Espionage)
- Physical Asset Theft

Role of the Malicious Insider:

For corporate espionage, the Insider is simply an agent assisting the main actors in executing their attacks. The insider may be motivated by any reason.
For physical asset theft the malicious insider can also be a main actor.



2.4.1 Strategy: Corporate Secret Theft

This is the case of corporate or industrial espionage. Any of the attackers are interested in stealing corporate secrets and other proprietary information. The rationale behind this may be different for each actor:

- The Nation State tries to obtain this data to improve the competitiveness of their own industries
- The Criminal sees an opportunity to monetize this theft in different ways
- The Hostile Investor gains an advantage by better understanding the company's strengths and weakness with respect to the larger markets they operate in
- The Competitor can leverage the data directly to improve their own products or strategies

2.4.2 Strategy: Physical Asset Theft

This is case of traditional theft of corporate resource. Typical attackers are criminals that try to enter company facilities and steal equipment, resources, or money. Malicious insiders are also main attackers, since they have very broad opportunities to steal from the company.

2.5 Scenario: Hostile Recruitment of Key Employees

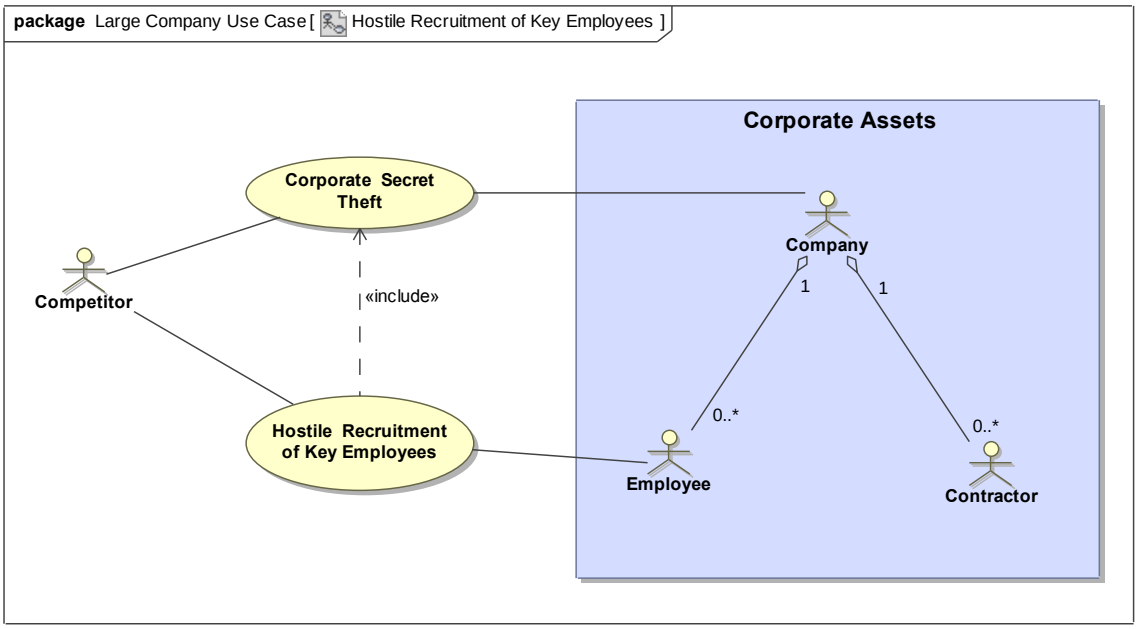
Main Actors:

- Competitor

Main Strategies:

- Hostile Recruitment of Key Employees

Role of the Malicious Insider:
The Insider does not play a special role in this scenario.



2.5.1 Strategy: Hostile Recruitment of Key Employees

The Competitor tries to hire key employees from the company to improve their own talent base and/or to diminish the talent base of the company. In doing so, the Competitor may also steal Corporate Secrets to identify key employees, better understand their contributions, and learn about their compensation packages.