Lab 2
Threat agent/threat modelling

Defining assets

Table 1. Information assets

Assets Name	Asset Background	Asset Category
Server, desktop, switch , router, connectors, hub	Physical infrastructure	Tangible
Cables, cell phone, T.V., DVD, storage devices	Physical infrastructure	Tangible
Articles, white paper, press release, music files, patent	Internet	Intangible
UPS	Physical infrastructure	Tangible
Application programs	Physical infrastructure	Tangible
Customer, employees' and suppliers' information (credit card, phone number, SSN#...), Website applications, inventory, supply and demand, marketing software	Internet	Tangible
copyright, survey data, trademarks, trade names, licenses, contracts, procedures, programs and procedures.	Internet	Intangible

Agent Attributes - a common set of characteristics that are used to define each agent uniquely. We settled on eight attributes: intent, access, outcome, limits, resource, skill level, objective, and visibility.

1. **Intent** - defines whether the agent intends to cause harm. Agents fall into two categories depending on their intent:

- **Hostile**: The agent starts with the intent to harm or inappropriately use assets, and the agent takes deliberate actions to achieve that result.
- **Non-Hostile:** The agent is friendly and intends to protect assets, but accidentally or mistakenly takes actions that result in harm.

Third category could be added - Environmental, to ensure that risk managers take into account uncontrollable and non-targeted threats occurring in the physical environment, such as fire, flood, pandemic, and military actions.

2. Access - defines the extent of the agents access to the company's assets. There are two options:

- **Internal**: Agent has internal access.
- **External**: Agent has only external access.

3. Outcome - usually defines the agent primary goal what the agent hopes to accomplish with a typical attack. However, with non-hostile agents, such as an untrained employee, the outcome may be unintentional. The agent may use many methods to achieve this goal, and the primary goal may have secondary or ancillary effects. Possible outcomes are:

- **Acquisition/Theft:** Illicit acquisition of valuable assets for resale or extortion in a way that preserves the assets integrity but may incidentally damage other items in the process.

- **BusinessAdvantage:** Increased ability to compete in a market with a given set of products. The goal is to acquire business processes or assets.

- **Damage**: Injury to personnel, physical or electronic assets, or intellectual property.

- **Embarrassment**: Public portrayal of unflattering light, causing to lose influence, credibility, competitiveness, or stock value.

- **TechnicalAdvantage**: Illicit improvement of a specific product or production capability. The primary target is to acquire production processes or assets rather than a business process.

4. Limits - these are the legal and ethical limits that may constrain the agent. This characteristic also defines the extent to which the agent may be prepared to break the law. Options are:

- **Code of Conduct:** Agents typically follow both the applicable laws and an additional code of conduct accepted within a profession or an exchange of goods or services. Example: an auditor falls within the Information Partner agent archetype.

- **Legal**: Agents act within the limits of applicable laws. Example: Legal Adversary.

- **Extra-legal, minor:** Agents may break the law in relatively minor, non-violent ways, such as minor vandalism or trespass. Example: Activist.

- **Extra-legal, major:** Agents take no account of the law and may engage in felonious behaviour resulting in significant financial impact or extreme violence. Example: members of organised crime organisations (Mobster agent).

5. Resource - defines the organisational level at which an agent typically works, which in turn determines the resources available to that agent for use in an attack. This attribute is linked to the Skill Level attributes a specific organisational level implies that the agent has access to at least a specific skill level. Options are:

- **Individual**: Resources limited to the average individual; agent acts independently. Minimum skill level: None.

- **Club**: Members interact on social and volunteer basis, often with little personal interest in the specific target. An example might be a core group of unrelated activists who regularly exchange tips on a particular blog. Group persists long term. Minimum skill level: Minimal.

- **Contest**: A Short-lived and perhaps anonymous interaction that concludes when the participants have achieved a single goal. For example, people who break into systems just for thrills or prestige (agent Cyber-Vandal) may run contests to see who can break into a specific target first. Minimum skill level: Operational.

- **Team**: A formally organised group with a leader, typically motivated by a specific goal and organised around that goal. Group persists long term and typically operates within a single geography. Minimum skill level: Operational.

- **Organisation**: Larger and better resourced than a Team; typically a company. Usually operates in multiple geographies and persists long term. Minimum skill level: Adept.

- **Government**: Controls public assets and functions within a jurisdiction; very well resourced and persists long term. Minimum skill level: Adept.

6. Skill Level: The special training or expertise an agent typically possesses. Options are:

- **None**: Has average intelligence and ability and can easily carry out random acts of disruption or destruction, but has no expertise or training in the specific methods necessary for a targeted attack.

- **Minimal**: Can copy and use existing techniques. Example: Untrained Employee.

- **Operational**: Understand underlying technology or methods and can create new attacks within a narrow domain.

- **Adept**: expert in technology and attack methods, and can both apply existing attacks and create new ones to greatest advantage. Example: Legal Adversary.

7. Objective - the action that the agent intends to take in order to achieve a desired outcome. Options are:

- **Copy**: Make a replica of the asset so the agent has simultaneous access to it.
- **Destroy**: Destroy the asset, which becomes worthless to either or the agent.
- **Injure**: Damage the asset, which remains in ownerâ€™s possession but has only limited functionality or value.
- **Take**: Gain possession of the asset so that owner has no access to it
- **Don't Care:** The agent does not have a rational plan, or may make a choice opportunistically at the time of attack.

8. Visibility - the extent to which the agent intends to conceal or reveal his or her identity. Options are:

- **Overt**: The agent deliberately makes the attack and the agent's identity is known before or at the time of execution.
- **Covert**: The victim knows about the attack at the time it occurs, or soon after. However, the agent of the attack intends to remain unidentified.
- **Clandestine**: The agent intends to keep both the attack and his or her identity secret.
- **Don't Care:** The agent does not have a rational plan, may make a choice opportunistically at the time of attack, or may not place importance on secrecy.

The Agents. To define the agents, we use an iterative process that began with a simple one sentence description of each agent. Our cross-functional team then progressively refined these definitions using the teams experience supplemented with outside references and expertise. Each agent has a unique set of attribute values, as shown in Table 1.

In addition to ensuring the uniqueness of each agent, this approach would enable risk managers to select relevant agents by first identifying the attributes that an agent must possess in order to represent a threat. We aimed to create agent definitions that were specific enough to be useful in risk assessments. For example, instead of defining a single agent to encompass all the current uses of the term hacker, we defined several different agents. One of these, Cyber Vandal, represented one original meaning of the term hacker: someone who intends to intrude into systems for thrills or prestige among peers. However, we also developed other real-world agents such as Data Miner, Internal Spy, Mobster, Government Spy, and Government Cyberwarrior to cover other agents that often are described using the umbrella term hacker.

The information that we provide to risk managers includes the matrix of agents and their attributes (as in Table 1) and a text-based summary reference list including brief descriptions of the agents, their common tactics, and current ratings, as shown in Table 2.

Some business units add environmental agents such as natural disasters and pandemics to the library of human agents, to ensure that assessors take them into consideration. However, providing more detail about these is beyond the scope of our group, so these business units must consult other resources, such as local authorities and security SMEs within the affected area, to characterise and assess those threats.

Table 2. Summary Agent Information

	Agent title	Common tactics/Actions	Descriptions
Hostile	Anarchist	Violence, property destruction, physical business disruption	Someone who rejects all forms of structure, private or public, and acts with few constraints
	Civil Activist	Electronic or physical business disruption; theft of business data	Someone who rejects all forms of structure, private or public, and acts with few constraints

	Competitor	Theft of IP or business data	Business adversary who competes for revenues or resources (acquisitions, etc.)
	Corrupt Government Official	Organizational or physical business disruption	Person who inappropriately uses his or her position within the government to acquire company resources
	Cyber Vandal	Network/computing disruption, web hijacking, malware	Derives thrills from intrusion or destruction of property, without strong agenda
	Data Miner	Theft of IP, PII, or business data	Professional data gatherer external to the company (includes cyber methods)
	Employee, Disgruntled	Abuse of privileges for sabotage, cyber or physical	Current or former employee with intent to harm the company
	Government Spy	Theft of IP or business data	State-sponsored spy as a trusted insider, supporting idealistic goals
	Government Cyberwarrior	Organizational, infrastructural, and physical business disruption, through network/computing disruption, web hijacking, malware	State-sponsored attacker with significant resources to affect major disruption on national scale
	Internal Spy	Theft of IP, PII, or business data	Professional data gatherer as a trusted insider,generally with a simple profit motive
	Irrational Individual	Personal violence resulting in physical business disruption	Someone with illogical purpose and irrational behavior
	Legal Adversary	Organizational business disruption, access to IP or business data	Adversary in legal proceedings against the company, warranted or not
	Mobster	Theft of IP, PII, or business data; violence	Manager of organized crime organization with significant resources
	Radical Activist	Property destruction, physical business disruption	Highly motivated, potentially destructive supporter of cause
	Sensationalist	Public announcements for PR crises, theft of business data	Attention-grabber who may employ any method for notoriety; looking for â€œ15 minutes of fameâ€
	Terrorist	Violence, property destruction, physical business disruption	Person who relies on the use of violence to support personal socio-political agenda
	Thief	Theft of hardware goods or IP, PII, or business data	Opportunistic individual with simple profit motive
	Vendor	Theft of IP or business	Business partner who seeks inside

		data	information for financial advantage over competitors
Non-hostile	Employee, Reckless	Benign shortcuts and misuse of authorisations, pushed wrong button	Current employee who knowingly and deliberately circumvents safeguards for expediency, but intends no harm or serious consequences
	Employee, Untrained	Poor process, unforeseen mistakes, pushed wrong button	Current employee with harmless intent but unknowingly misuses system or safeguards
	Information Partner	Poor internal protection of company proprietary materials	Someone with whom the company has voluntarily shared sensitive data

Exercises

Task 1. For each agent find unique set of attribute values (MS Excel "Task 1").

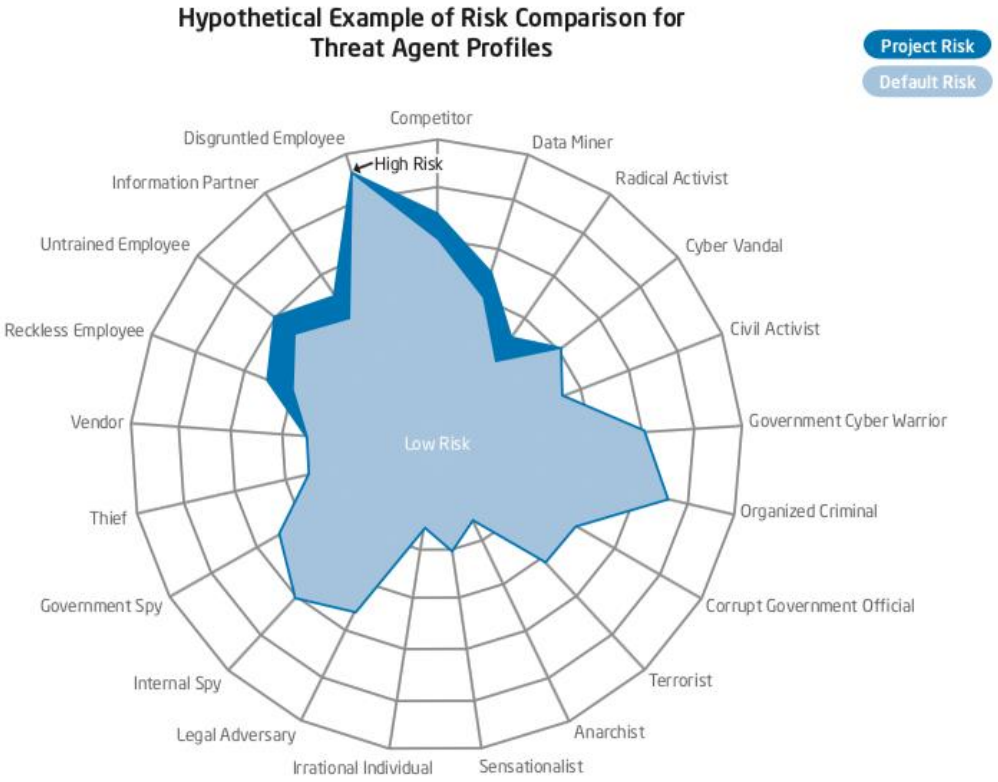
Task 2. Finish the table by identifying threats for each asset

Assets	Threats														
	Firmware Modification	Traffic Sniffing	Hardware Modification	Unauthorized physical access/entry	Loss of Compliance	Modification-of-Service	Denial of service attacks (DoS/DDoS)	Violations of law or regulation/breaches of legislation	Address space hijacking (IP prefixes)	Unintentional damages (accidental)	Social engineering	Identity theft	Malware and viruses	Loss of reputation	Compromising confidential information (data breaches)
Server, desktop, switch, router, connectors, hub	0.7	0.8	0.1	0.2	0.5	0.1	0.6	0.2	0.1	0.2	0.1	0.8	0.8	0.2	0.1
Cables, cell phone, TV, DVD, storage devices	0.1	0.8	0.6	0.1	0.1	0.5	0.3	0.1	0.0	0.4	0.2	0.2	0.0	0.6	0.4
Articles, white paper, press release, music files, patents	0.2	0.1	0.2	0.4	0.4	0.3	0.5	0.2	0.1	0.4	0.3	0.4	0.2	0.1	0.2
UPS (uninterruptible power source)	0.2	0.2	0.3	0.2	0.1	0.2	0.1	0.1	0.1	0.4	0.1	0.1	0.1	0.1	0.1
Application programs	0.5	0.7	0.1	0.5	0.5	0.5	0.6	0.6	0.2	0.4	0.2	0.1	0.8	0.1	0.2
Customer, employees' and suppliers' information (credit card, phone number...), web applications, inventory, supply and demand, marketing software	0.7	0.8	0.1	0.5	0.5	0.5	0.4	0.4	0.1	0.2	0.8	0.7	0.7	0.2	0.5
Copyright, survey data, trademarks, trade names, licenses, contracts, procedures, programs and procedures.	0.2	0.1	0.1	0.1	0.3	0.1	0.1	0.8	0.5	0.5	0.5	0.3	0.2	0.1	0.2
Server, desktop, switch, router, connectors, hub															

Task 3. Finish the table by estimating likelihood of attack: from 0 to 1. Calculate probability of attack by each threat agent. Show result using chart as you can see below.

Threat agents	Threats														
	Firmware Modification	Traffic Sniffing	Hardware Modification	Unauthorized physical access/entry	Loss of Compliance	Modification-of-Service	Denial of service attacks (DoS/DDoS)	Violations of law or regulation/breaches of legislation	Address space hijacking (IP prefixes)	Unintentional damages (accidental)	Social engineering	Identity theft	Malware and viruses	Loss of reputation	Compromising confidential information (data breaches)
Employee Reckless	0.8	0.1	0.2	0.2	0.5	0.6	0.1	0.5	0.1	0.5	o.2	0.4	0.5	0.5	0.6
Employee Untrained	0.8	0.2	0.5	0.2	0.5	0.7	0.2	0.5	0.2	0.7	0.2	0.2	0.5	0.2	0.2
Info Partner	0.7	0.1	0.2	0.2	0.5	0.5	0.1	0.5	0.2	0.5	0.2	0.5	0.5	0.5	0.2
Anarchist	0.5	0.2	0.1	0.2	0.4	0.5	0.5	0.6	0.1	0.3	0.7	0.2	0.4	0.1	0.1
Civil Activist	0.7	0.2	0.1	0.5	0.5	0.5	0.5	0.6	0.5	0.6	0.1	0.5	0.4	0.5	0.4
Competitor	0.6	0.2	0.1	0.6	0.6	0.5	0.3	0.3	0.2	0.4	0.1	0.6	0.5	0.6	0.5
Corrupt Government Official	0.6	0.4	0.1	0.6	0.5	0.4	0.3	0.3	0.7	0.6	0.2	0.5	0.5	0.4	0.4
Data Miner	0.7	0.6	0.2	0.5	0.5	0.6	0.5	0.3	0.3	0.6	0.1	0.6	0.4	0.3	0.5
Employee Disgruntled	0.5	0.4	0.1	0.3	0.3	0.2	0.2	0.5	0.4	0.3	0.2	0.3	0.3	0.2	0.3
Government Cyberwarrior	0.7	0.6	0.2	0.5	0.6	0.4	0.6	0.6	0.7	0.4	0.2	0.2	0.5	0.1	0.1
Government Spy	0.7	0.5	0.1	0.6	0.5	0.3	0.5	0.5	0.6	0.4	0.1	0.5	0.5	0.2	0.2
Internal Spy	0.6	0.3	0.2	0.5	0.4	0.2	0.5	0.5	0.6	0.3	0.2	0.5	0.4	0.2	0.1
Irrational Individual	0.5	0.2	0.1	0.4	0.3	0.2	0.4	0.3	0.4	0.2	0.1	0.3	0.4	0.1	0.1
Legal Adversary	0.4	0.2	0.1	0.3	0.2	0.1	0.3	0.2	0.3	0.2	0.2	0.3	0.3	0.1	0.2
Mobster	0.4	0.2	0.2	0.3	0.2	0.1	0.2	0.2	0.2	0.1	0.1	0.4	0.3	0.2	0.3
Radical Activist	0.3	0.3	0.2	0.2	0.1	0.1	0.2	0.1	0.1	0.2	0.2	0.2	0.3	0.2	0.2
Sensationalist	0.4	0.1	0.1	0.2	0.1	0.2	0.2	0.2	0.1	0.1	0.1	0.2	0.3	0.1	0.2
Terrorist	0.7	0.5	0.3	0.6	0.6	0.4	0.5	0.6	0.7	0.3	0.2	0.5	0.7	0.1	0.3
Thief	0.7	0.6	0.2	0.5	0.5	0.6	0.4	0.5	0.6	0.2	0.1	0.4	0.6	0.2	0.3
Vandal	0.5	0.3	0.1	0.3	0.2	0.2	0.2	0.3	0.4	0.1	0.1	0.3	0.4	0.2	0.2
Vendor	0.6	0.4	0.1	0.4	0.5	0.2	0.3	0.6	0.4	0.2	0.2	0.5	0.5	0.1	0.3

Result:


Hypothetical Example of Risk Comparison for Threat Agent Profiles
Project Risk
Default Risk
Competitor
Data Miner
Radical Activist
Cyber Vandal
Civil Activist
Government Cyber Warrior
Organized Criminal
Corrupt Government Official
Terrorist
Anarchist
Sensationalist
Irrational Individual
Legal Adversary
Internal Spy
Government Spy
Thief
Vendor
Reckless Employee
Untrained Employee
Information Partner
Disgruntled Employee
High Risk
Low Risk

Task 4. Finish the table by estimating the influence of each security measure on threats from 0 to 5 (5 – security measure fully prevent attack, 0 – security measure is useless against threat)

Security measures	Threats														
	Firmware Modification	Traffic Sniffing	Hardware Modification	Unauthorized physical access/entry	Loss of Compliance	Modification-of-Service	Denial of service attacks (DoS/DDoS)	Violations of law or regulation/breaches of legislation	Address space hijacking (IP prefixes)	Unintentional damages (accidental)	Social engineering	Identity theft	Malware and viruses	Loss of reputation	Compromising confidential information (data breaches)
Identification and Authentication	0	1	1	5					2		3	2	2		3
Access Control					2		1								
Security intelligence systems	2	2		4											
perimeter controls			2	5				1		2		2			1
encryption technologies					1			1				2		2	4
Automation, orchestration and machine learning	2						3								
Firewalls															
anti-virus protection													5		
Intrusion detection system	3	5	2			3	2		5			2	3		3
Internal or IT audit					5			4						4	
Employee training								2		4					
CCTV				4											
Incident response team	1	3	2	3											

Digital forensics															
distributing keys to intended users							3		3						
legal considerations, for example requirements for electronic signatures;					4			3							4
Audit logs: userIDs; dates, times, and details of key events, e.g. log-on and log-off;	3	3				3									
password management system						3									4
clear desk policy			2										2		2
alarms				4											