**Case: Theft of Intellectual Property**

**Team Members and Job Roles**

1. Sabeet C.- Information Security Officer

2. Akshar P. - IT Risk Analyst

3. Hrishav A. - IT Risk Analyst

4. Jimmy Q. - Behavioral Analyst

5. H M Bayezid - Compliance Analyst

6. Will P - Cyber Threat Analyst

7. Abu Rajib - cyber Threat Analyst

**1.Understand the case and summarize it:**

* Who was the threat-actor
* Pangang coders
* Root cause of problem
* Trusted US contractor gave trade secrets to Pangang coders to steal financial platform and design
* How do you prioritize what to do first
* Find the culprit, fire him and report him for intellectual theft.
* Who do you report the incident to

- National Intellectual Property Rights Coordination Center (NIPRCC) and the FBI

**2. How do you communicate to the business units.**

- In this case, it is important to restructure and recreate a new financial model as the Chinese have a competitive advantage over us.

**3. What’s the messaging you provide to business units. How about the executives.**

- We tell the executives the importance of what happened, what needs to be fixed in order to save billions of dollars by spending a few millions on a new platform. We need to make security tighter and give out big punishments to any offenders.

**4. What would be the messaging for the public if the impact was to a key public facing business process.**

- Gain the trust of the public by severing ties with all offending parties. Make many apologetic statements. Tell them we are working with third parties and the FBI to make sure nothing like this ever happens again

**5. Findings.**

**-** Our findings showed us our vulnerabilities and the fixes that we have to make and restructure our security for the sake of our trade secrets

**6. What laws are in place to convict the threat actor.**

- The FBI and the NIPRCC are able to

* Criminal fines
* Imprisonment for several years, depending on the nature of the charges
* Seizure of the stolen property, documents, or materials
* Loss or suspension of a business operating license
* Civil charges filed by the victim of the crime (for instance, for lost business profits)

**7. What controls / security measures should be implemented to prevent a repeat.**

- Physical security keys such as USB flash drive keys to allow for two step authentication to prevent unauthorized access

- Heavily monitor each individual internet traffic to see if a person is speaking to a rival company

- Monthly audit of each employees interaction with foreign nations

**8. Recommendations.**