Certain information must be available for analysis for relevancy of intelligence or threats to an org. The information required is the answers to the following questions. The information includes data from other internal organizations, research already performed, researched to be performed, including open source collection:

* What data do we create and maintain that is of importance to the company? What laws protect that data?
* Where is that data located? How would we be impacted if it was discovered, distorted, disrupted, destroyed?
* What data do we obtain from clients that are of importance to the company? What laws protect that data?
* Where is that data located? ? How would we be impacted if discovered, distorted, disrupted, or destroyed?
* What products created, delivered, and supported by our suppliers are the most critical to the company's success?
* Where are they created, and by whom? What companies create what components that make up each of the critical products? Where is the IP around those products stored?
* What software created, delivered, and supported by us and our suppliers are the most critical to the success of the company
* What software created, delivered, and supported by us and our suppliers are the most critical to the success of the company
* Where is the software created, and by whom? What companies create what software that makes up each of the critical products? Where is the data relative to those products stored?
* Who has executed cyber-attacks on us in the past? Who has executed cyber-attacks against others in our industry in the past? List them all out by type, intent, motivation, skill, sophistication, etc.
  + When was the last time each attacked?
  + How many times did each attack?
  + Were they successful?
  + What did they achieve?
  + Did they target any of the IP, PII, or critical products described above?
* What adversaries are most likely to want our intellectual property, and why?
* What adversaries are most likely to want the PII that we hold and why?
* What would adversaries achieve by targeting and exploiting our hardware supply chain?
* What would adversaries achieve by targeting and exploiting our software supply chain?
* What is the current defensive/security posture of the organization?
* What are the SWOTs of that posture? (Strengths, Weaknesses, Opportunities, Threats)
* What gaps do we have in people, process, and technology?
* What is considered the (or are considered) the weaknesses – the least path of resistance in our security stack (people process technology)
* What threat actor attributes would exploit the weaknesses as described above?
* If exploited, what data would the attacker access?
* Who would gain competitively if their nation's hacking apparatus targeted us and shared the fruits of the attack with their like-industries

# Company Baseball Card

|  |  |
| --- | --- |
| Company Name and Major Brands |  |
| Major lines of business and industry sector | *Examples:*  *Biomedical Research – Healthcare Research*  *Medical Services – Healthcare services*  *Compounding and small molecule development – Pharmaceutical* |
| Geolocations of major centers for the company |  |
| Geopolitical or social statements or stances made by the company |  |
| Crown Jewel data |  |
| Crown Jewel applications |  |
| Crown Jewel products critical to company success |  |
| Describe how the value chain moves through the company  Where does money come in, and leave your org and what is required for that transaction? | *Examples:*  *Insurance claims paid by payer services*  *Wellness Benefits gift cards to employees*  *Payments by patients for services and co-pays – cash, credit card / credit card processing by Card Services Inc*  *Laboratory testing services*  *Payments to vendors and third-parties on invoices* |
| What do we look like to attackers? What does OSINT on ourselves show? | *Examples:*  *Attack Surface – shodan*  *Subdomains – cert.sh*  *Job postings – technology, projects, etc*  *New releases – M&A, geopolitical, social characterization*  *Social Media – exposed VIPs, clear targets to value chain* |
| Rhythms of business – what is a busy time and why?  *This tells you what events or times the company maybe most likely to be social engineered*  *Typically, you can discover many of these by looking at spikes in searches or internet traffic for your org* | *Examples:*  *Annual enrollment – September every year*  *M&A activities*  *Large disasters, medical crisis* |
| Third-party relationships | *Examples:*  *Key software*  *Key hardware*  *Key supply-chain vendors*  *Key third-party relationships whose disruption would disrupt our org* |
| Previous incidents root cause and MITRE ATT&CK TTPs observed |  |
| Previous incidents threat actors’ attribution |  |
| What is our security control posture? | *Typically expressed in MITRE ATT&CK matrix based on purple team activities to validate security controls* |
| SWOT analysis | *What part of the MITRE ATT&CK TTPS were observed in incidents that security controls were insufficient and why*  *What part of the MITRE ATT&CK TTPS were observed in incidents that security controls were sufficient and do we know that to be consistent across assets or not?* |