INTERVIEW NOTES

Interviewers	Eric Marinho da Silva, Veeraiah Nannapaneni, Jill Navarro, Jessica Romio, Rand Shamas, Melissa Svoboda
Participants:	Government End-User (G-EU), Government Information Technology Manager (G-IT), Manufacture Business User (M-BU), and Manufacture Information Technology Manager (M-IT)
Date:	March 20, 2020
Location:	University of San Diego (CSOL-560)

INTERVIEW 1: GOVERNMENT USER

Q1. Who will access the system, and how will that access be secured?

G-IT: The manufacturers and government required system via Azure Active Directory (AAD) business-to-business (B2B). AAD integrates with on-premises Active Directory to provide Seamless Single Sign-On (Seamless SSO), and secure user accounts with multi-factor authentication (MFA) for all Tracker Analytics users. Access control for least-privilege configurations and user activity must be tracked, logged, and revoked if necessary.

G-EU: Suppliers and shipment companies must have limited access.

Q2. What information do you need to view on the dashboard?

G-EU: View real-time transportation routes that reduce risk caused by natural hazards and erroneous or malicious acts. Facility location for shipment and delivery.

G-IT: Real-time cyber threat intelligence for the manufacturing facility, distribution centers and routes, quality control, logistics, and satellite imagery.

Q3. How will the information be displayed on the dashboard be gathered?

G-IT: We need to pull the data from the Fusion Engine and integrate with Scout Severe Weather data, and Google Maps API. Additionally, we need external cyber threat intelligence feeds to show real-time risk-related information on suppliers, their distribution channels, and assets.

Q4. What information is required to track/monitor the manufacturers, assets, and asset transportation?

G-EU: Manufacturer, destination locations, weather, GPS, packing data, shipping data, receiving data, and asset inventory data.

Q5. What type of asset location notification is required?

G-EU: Real-time tracking of the asset. Notification when an asset changes vehicle, notification when the asset crosses state or borderlines, route changes, and notification if an unusual event occurs

G-IT: Based on machine learning models.

Q6. How should the tracking analytics system communicate with other systems?

G-IT: Data travels through API gateways, through a stream processor to a database, and then displayed onto the dashboard.

Data must be secured by relying on NIST AC-4 Information Flow Enforcement control policies to have a clear picture of how information moves within the system and between systems.

Keep data from being transmitted to the internet, block outside traffic from being allowed into the system, restricting information transfer between security domains, secure architecture between interconnected systems.

Additionally, we need restful API integration, HTTPS, AAD, SSO, and MFA.

Q7. How are weather-related delays or natural disasters handled?

G-IT: As weather data is gathered, alerts are displayed on the dashboard. Google maps then re-routes assets.

Q8. Do routes need to be changed in the case of natural hazards or malicious acts?

G-EU: Yes, if the hazard or act will cause harm or delay to the asset.

Q9. What are the ramifications if the tracking analytics system fails?

G-EU: If the tracking analytics system fails, our assets may be used for malicious acts.

A delay will also cause insufficient supplies for combat situations.

Q10. How will the system be automated?

G-IT: Use artificial intelligence and machine learning models for risk prevention and mitigation.

Q11. What is a logical manner to separate system requirements in the case of a modular failure?

G-IT: Each module and third-party vendor will provide information through the fusion engine and into the tracker analytics. Therefore, one failed module will not cause other modules to fail.

Q12. How long does the data need to be retained?

G-EU: Up to 20 years. The data will be stored within a secured repository.

Q13. When does the system need to be available?

G-IT: Twenty-four hours and 365 days a year.

Q14. What platforms does the tracker analytics system need to be available on?

G-IT: Computers and mobile devices. No application installation required. The tracker analytics system must be a web-based application and, therefore, be available on any platform.

Q15. How is confidential/secure data to be handled?

G-IT: Policies and procedures exist for classifying data. Data is encrypted based on its classification.

Q16. What's your budget to perform integrations for the tracking analytics?

G-IT: $400,000.00 over three years.

INTERVIEW 2: CONTRACT ELECTRONICS MANUFACTURER (CEM)

Q1. How do you securely connect to the distribution centers, logistics, and shipment routes databases? Do you have their addresses, pricing, and supply asset inventory?

M-IT: We encrypt connectivity with the databases via SSL. Access to encryption keys requires the use of a key management solution, and we store and manage the encrypted keys.

M-BU: Yes, we have addresses, pricing, and asset list of inventories available as well as access to other distributors and logistics vendors in case supply runs low.

Q2. Do you require suppliers and logistics supply chain to follow regulations such as International Traffic in Arms Regulations (ITAR)?

M-BU: Yes, based on government regulations, suppliers, and logistics, vendors need to be ITAR certified.

Q3. How do you require/support the external systems to connect to databases?

M-IT: We support secure both cloud-based and on-premises connectivity with RESTful API over SSL.

Q4. How do you want to be notified and alerted? Real-time?

M-BU: Real-time notification on a dashboard and tracker map is critical to keep track of supply inventory, cost volatility, disasters, malicious acts, and shipment routes.

Shipping drivers need to be alerted of any natural disasters in routes or malicious events.

Q5. How do you manage the tracking inventory of products made and transported? Are sensors used throughout the production process? Are serial numbers used?

M-BU: Due to the sensitivity of our products, we use GPS and inventory tracking sensors throughout the product life cycle with unique serial numbers, until the product is delivered.

Q6. What tracking mechanisms are available to track locations, routes, suppliers, and shipment?

M-IT: GPS is used for tracking.

Q7. Do you need integration with external applications like quality control, logistics intelligence, satellite imagery, and human intelligence for additional visibility?

M-BU: Yes, integrations are essential to all those intelligence-built databases to make sure we have full visibility on our products up until delivery. Tracking analysis needs to be used to alert on any abnormalities and provide real-time metrics.

Q8. How do you avoid mistakes and malicious acts during shipment and delivery?

M-IT: Integration with intelligence databases based on machine learning models and GPS tracking are good ways to avoid those human or malicious acts.

Q9. Do you require real-time risk-related information about your distribution channels and suppliers?

M-BU: Yes, it is essential to keep inventory supply up to date at our distribution centers and with the suppliers.

Q10. Do you require real-time transportation routes information to reduce risks and mitigate damage due to natural or human-made hazards?

M-IT: Yes, it's crucial to have real-time GPS tracking mechanisms and intelligence-built on machine learning models so our distributions centers, suppliers, and logistics are on alert for such hazards.

Q11. Do you require integration with a cyber-threat information feed for the supply chain?

M-IT: Yes, such real-time integration will help identify cyber threats that may impact product manufacturing with hardware and software vulnerabilities to update them before our customers receive them.

Q12. Are there any restrictions to host a system, or web-based portal, in the cloud instead of an on-premises infrastructure?

M-IT: No, as long as it complies with the government policies. As part of our digital transformation initiatives, we are moving towards a cloud-first infrastructure.

Q13. Are there any guidelines for handling confidential data/security?

M-IT: Only authorized users should access the tracker analytics portal using single-sign-on and multi-factor authentication. Our users and customers should have access to this portal based on their roles and responsibilities

Q14. Are there any requirements to access your shipping portal?

M-BU: Yes, only our customers and our users should have access to it, and no one else.

Q15. Are steps taken to "tamper-proof" products?

M-BU: All of our products come with sensors to track configuration changes and GPS location. Only authorized personal with high clearance will have access to our products. We follow government guidelines and security industry best practices – ISO/IEC 27001/27002, NIST 800-53, 161, 171

Q16. Who needs access to the tracking analytics system? What are their roles? How often will they be audited for validity?

M-BU: Suppliers, manufacturers, customers. Logistic roles must have limited access.

M-IT: Auditing and logging should be enabled on the tracking system and sent a SIEM for events logging and forensics. A quarterly auditing is sufficient.