Security in the Supply Chain

Presented by

Heather Nickerson
EVP and CFO
Red Five Privacy Labs, LLC

Paul Kurtz
Co-Founder and CEO
TruSTAR

TRUSTAR

6 March 2019

Objectives

- Explain the step-by-step process of the physical and digital aspects of a supply chain investigation
- Learn how to better leverage the digital aspects

Agenda

- Case study example to showcase the five-step process
- Q&A

Case Study

- An electronics manufacturer is negatively affected by the sale of knock-offs being created from parts siphoned off of different links in the supply chain.
- The manufacturer’s reputation, supply chain, and bottom line needs to be protected.
- An investigation must be considered as an information gathering effort and mitigation path.

Step 1: Understand

- What's the investigative objective?
- Decide whether to investigate
- Understand the resources, physical effort and potential outcomes/impact of the investigation
- Understand the ROI
- What internal systems do you use to flag and manage suspicious activity?
- Which systems are associated with fraud and abuse?
- Are you cognizant of the status of systems associated with your supply chain?
- Consider an enterprise intelligence requirements officer

Step 2: Collect

- Begin to collect potential physical and digital evidence
- Digital information can help narrow the physical search and collection
- Consider how the collected data is protected, how it can be shared, and how it is anonymized
- Aggregate and normalize data sets in permissions-based data repositories
- Add external threat data from government or private sources
- Integrate internal and external data sets
- Inform supply chain partners about your approach

Step 3: Analyze

- Connect the dots alongside what you have as internal knowledge
- Identify new leads based on analysis
- Make decision on next steps and whether investigation is overt or covert

- Affordable software solutions can expedite analysis and break down silos
  - Search engines
  - Different personnel can add data points
  - Automatically update case management systems
- Evaluate the evidence
  - Utilize internal data for source validation
  - Case management discipline
  - Be careful of scoring algorithms

Step 4: Take Action

- Once case is built, consider the presentation and audience
- Coordinate internally across multiple departments, and consider potential outcomes
- Permissions-based access is critical
- Arrange access to data based on function
- Monitor access and logging

Step 5: Follow Up

- Monitor and remediation
- Lessons learned
- Increased participation in micro-exchanges, particularly in the supply chain community

Questions?