Food Defense Consortium

Evolving Threats

Robert A. Norton, Ph.D.

Auburn University

Email: nortora@auburn.edu

Disclaimer: The following presentation represents the personal opinions of the presenter and does not reflect the official views or statements of Auburn University, the State of Alabama or the federal government and it constituent agencies.

Food Defense – A Holistic Strategy

- “Farm to Fork”
- Food production as a complex “system of systems” – Inputs and Outputs
  - The disruption of which can cause “cascading effects”
  - Rapidly cross sectors – cyber/electrical/water/food processing
- Agriculture and Food as Critical Infrastructures sectors as defined by Presidential Policy Directive 21 (PPD-21).
  - “…whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.”

Food and Agriculture Sector

- Cybersecurity and Infrastructure Security Agency (CISA):
  - The Food and Agriculture Sector is almost entirely under private ownership; estimated 2.1 million farms: 935,000 restaurants: more than 200,000 registered food manufacturing, processing, and storage facilities.
  - This sector accounts for roughly one-fifth of the nation's economic activity.
  - “Critical Dependencies”:
    - Water and Wastewater Systems, for clean irrigation and processed water
    - Transportation Systems, for movement of products and livestock
    - Energy, to power the equipment needed for agriculture production and food processing
    - Chemical, for fertilizers and pesticides used in the production of crops

Food Defense – An Intelligence Problem

- Intelligence – Ordered and validated information that can provide decision makers with fact and context.
- Beyond the regulatory requirements, there is a need for understanding both the threat actors and the threats they offer.
  - Constantly evolving
  - Constantly responding to defensive postures
  - “Thinking adversaries”
- Timeliness of information is essential for effective decision making.
  - Stale information is your enemy, not your friend.
- Evidence of due diligence.
- Protects brand, physical assets and personnel.

What does the adversary see?

- Context: A “target rich environment”
  - Many opportunities for malevolent activities
  - Social unrest and violence
  - Major social, financial and business disruptions from COVID
  - Psychological stress and emerging mental illnesses (e.g. depression, suicide, etc.)
    - Angry, confused, frightened, feeling threatened
  - Brewing political disunity – coming election
- Who is the adversary?
  - A spectrum of adversaries
    - **Disgruntled employees (high probability/relatively lesser impact)**
    - Criminal groups and individuals (high probability/high impact)
    - Hacktivists (increasing probability/moderate to high impact)
    - Nation States (low probability/high impact)
- **Whoever the adversary or their motivation – assume they are “inside the wire”**

Intelligence Findings and Conclusions:

- “The current threat spectrum is significantly affected by social disruption in multiple forms (e.g. COVID; demonstrations; riots), increasing the likelihood of escalating malign activities from criminal organizations and nation states in the weeks leading up and subsequent to the Presidential election in November…regardless of who wins….foment instability…”
- “Nation states are actively seeking to exploit unrest and foster conflict…”
- “Criminal organizations/nation states are currently very active in the cyber realm…This is expected to significantly increase prior to the Presidential election…Major disruptions are possible…”
- “Increased social, psychological/mental health and financial pressure is significantly increasing the probability of disgruntled employees and insider threats…possibly increasing the likelihood of violence…”

Intelligence Findings and Conclusions (cont.)

- "…Coalescing of activism with increased radicalism, including groups that promote and carry out violence…"
  - Anti-government
  - Anti-corporate
  - Anti-capitalist
  - Well financed and organized
  - Communist with connectivity (China, Russia, North Korea, Cuba, Venezuela)
- Anarchist Groups utilizing Black Bloc tactics
- Animal Rights/Radical Ecological reemerging
  - Some promoting "direct action"
- "A radical is a radical is a radical…" - Connectivity, training and coordination
- **These individuals and groups may eventually target your facilities, brand, products and/or personnel.**
- Why? The food supply supports economy, overall well-being and national stability…You are viewed as "Corporate America"

Solutions

- Intelligence: a process; infrastructure and personnel.
- To facilitate the dissemination of timely Intelligence, Critical Infrastructures (CIs) have created Information Sharing and Analysis Centers (ISACs).
  - Government and Business working in partnerships
  - Provide a pipeline for communication
  - Identify threats and develop solutions
  - Train
  - Intermediaries/advocates with regulatory agencies
  - Evolve Intelligence activities as threats/actors change