Cyber Security Summit International Breakout
October 27, 2020

The world is changing at a pace that has outstripped many of our institutions capacity to adapt. The fundamental ambition of this two-part session was to create a relevant event that demonstrated that reality to the audience. The interactive program sought to provide attendees with access to cutting-edge thought at a time when global supply chains are experiencing radical upheaval.

By forcing the Cyber Security Summit online, Covid-19 limited the session's ability to create a truly interactive experience, especially during the second half. The wargame was impacted by an absence of a physical audience and an online infrastructure that impeded the free flowing of information. Despite these challenges, the event was a success and serves as a blueprint for a time when we can gather, elucidate and shake one another's hands once again.

The following report details the threats and vulnerabilities facing global supply chains in the years to come with analysis and contribution provided by some of the industry's sharpest horizon scanners and innovators.

This session was facilitated by a team of volunteer graduates who served as rapporteurs and logistical support staff. At a difficult time for our younger generation, they gave up their free time to work as liaisons between team members, session staff and event leadership. They also helped translate the session into text that was formed into this report. Our sincere thanks go out to them.

Program Co-Chair and Host:
Michelle Greeley, Sr. Director, Global Risk Management, CWT

Program Co-Chair:
Anne C. Bader, Founder International Cybersecurity Dialogue, LLC

Chief Rapporteurs:
Simon Bracey-Lane, Research Fellow, Institute for Statecraft

Rapporteurs:

- Sherwin Bothello.
- Alyssa Chetrick.
- Alex Gilbertson.
- Tanner Manley.
- Sheila Padre.

The annual theme of this year's Cyber Security Summit was 'The Ripple Effect' – a reflection of the cascading impacts that we constantly have to manage in our field to stay ahead of threats.

The International Program of the 2020 Cyber Security Summit consisted of two sessions that examined emerging threats to global supply chains in a post COVID-19 world.

The first session was a briefing by Interos CEO and Founder, Jennifer Bisceglie. She detailed her organization's shift to using emerging technologies to better prepare businesses for geopolitical disruption. She was joined by Expert Commentators: Mary Frantz, Chief Information Security Officer, Prescryptive Health, Inc. and Founder, Enterprise Knowledge Partners, LLC and Mark Ritchie, President, Global Minnesota; U.S. Army; State of Minnesota.

The second, led by Dr. Lynette Nusbacher, Principal at Nusbacher Associates was an interactive session that tasked two teams with attacking a global food supply chain. Using a graphical representation of a supply chain produced by FPDI's CRISTAL supply chain simulator, Dr. Amy Kircher, Co-Director of the Food Protection and Defense Institute (FPDI) University of Minnesota, outlined the scenario for the teams.

Team 1:

1. Brian Isle, Senior Fellow UMN Technological Leadership Institute
2. Mike Kearn, Director, Threat Informed Defense at U.S. Bank
3. Jennifer Reicherts, Threat Hunter and OSINT expert
4. Andrew Crocker, CEO, P2020ACADEMY
5. Pekka Vepsäläinen, CEO, Tikkasec Ltd.
6. Chad Svihel, Executive Director, Minnesota, PCs for People

Team 2:

1. Todd Carpenter, Chief Engineer and Owner at Adventium Enterprises
2. Justin Opatrny, Sr. Manager, Cyber Security – Supply Chain
3. Richard Stiennon, Chief Research Analyst, IT-Harvest
4. Wendy Foslein, Lead Data Scientist, Thermo King
5. Stephen Streng, Food Defense Analyst, FPDI

The following report details the two sessions. It will offer insights on the future of supply chain security through a presentation by a supply chain CEO of how today's supply chain operates: its improvements and its vulnerabilities with expert commentary by experts in Part I followed by a live demonstration of a horizon scanning exercise that weaves business strategic thought, exploration of supply chain vulnerabilities, attack surfaces and defense tactics in Part II.

International Breakout Part One: Deep Dive into the Global Supply Chain: Risk, AI and Data Analytics

With a staggering over-reliance on overseas exports, Covid-19 exposed the fragility of our complex and heavily optimized supply chains. This has caused significant declines in national GDPs, a third of the global economy came to a halt and unemployment has increased immensely. It is difficult to have a truly resilient supply chain that is optimized for shocks like this pandemic. Many organizations are aware of who they are supplied by, but not necessarily who supplies their suppliers. Interos addresses this problem by developing the world's largest, AI driven, business relationship graph.

Interos, a supply chain and vendor risk consultancy, uses a revolutionary approach to third party risk management. It uses artificial intelligence to map out global supply chains to identify potential supply vulnerabilities. The pandemic has meant that analysis of the global economy and global supply chain is more important than ever. It has been a shock that has prompted companies to take a closer look at risks within every tier of the supply chain. It has also illustrated a need for real systemic change within the international business community.

Many companies typically know which suppliers they are directly connected to. However, in the post-COVID 19 world it is vital to possess a deeper understanding of your supply chain. Knowing the risk factors that might impact a multi-tier supply chain, if your business is heavily reliant on a specific part of the world, disruption there could prove costly. This kind of understanding is vital if organizations are to grasp the risks present in the modern global supply chain.

Businesses need to be aware of what they are dependent on. They must develop the capability to anticipate disruptions in the supply chain and scan the horizon for what is occurring in the world. This means not only looking at the supply chain from a linear perspective but also a horizontal and vertical one because businesses need to try and get ahead of that ripple effect.

Organizations need to simultaneously be conscious of their geographical vulnerabilities and possess the drive to innovate to avoid the dangers that come with overreliance. Circumventing concentration risk, companies must find alternative suppliers to satisfy their supply chain needs.

Companies can apply human subjectivity to AI solutions to build operational resiliency and make better-informed decisions in the post-COVID 19 world. By leveraging AI, businesses can increase their visibility of business relationships and dissipate uncontrolled supply chain risks and threats. In addition, businesses can source alternative suppliers and know where to apply their resources and investment.

International Breakout Part 2: Securing the Global Supply Chain through Red Team Analysis.

Global food supply chains will be compromised in the post COVID-19 world. Companies must adjust to survive and thrive. Despite businesses' efforts to procure security solutions, they will remain vulnerable from the interconnectivity of modern supply chains and the interactive relationship between attackers and defenders.

This risk landscape is constantly evolving. This ensures existing and more static strategies will be threatened. There will be a direct struggle between attackers and defenders. If defenders do not foresee and adapt to these interactive attacks, their systems will be at risk.

In food supply networks, multiple consumer and businesses' systems interact. The interconnectivity of this system is akin to fabric, sewn together. When pulled, if the stitch is too strong it will tear the fabric, if the fabric is too strong the stitch will tear. A balance between the two must be achieved.

We must recognize that our systems were developed in a "different world". The illusion of normalcy must be dispelled. COVID-19 must be a wake-up call. To recognize the vulnerability of our interconnectivity and interactivity systems, how our domestic world can be impacted.

The Task

Two red teams were presented with supply chain information from a fictitious seafood company that manufactured breaded shrimp. A graphical simulation of the supply chain detailing movement from source to consumer was presented. Both teams were tasked with developing a multi-stage attack strategy that involved:

- **Identifying critical assets:** essential entities within the supply chain of a company which if attacked or disabled could significantly hinder the overall supply chain.
- **Assessing key attack surfaces:** The number of key methods where an attacker can attack an associated asset and compromise it.
- **Identifying vulnerabilities:** What can be exploited, ties into attack surfaces; is the weakness which can be exploited by an attacker.
- **Optimum attack scenario:** Electing which method will be most effective and including a brief summary of the exploitation process.

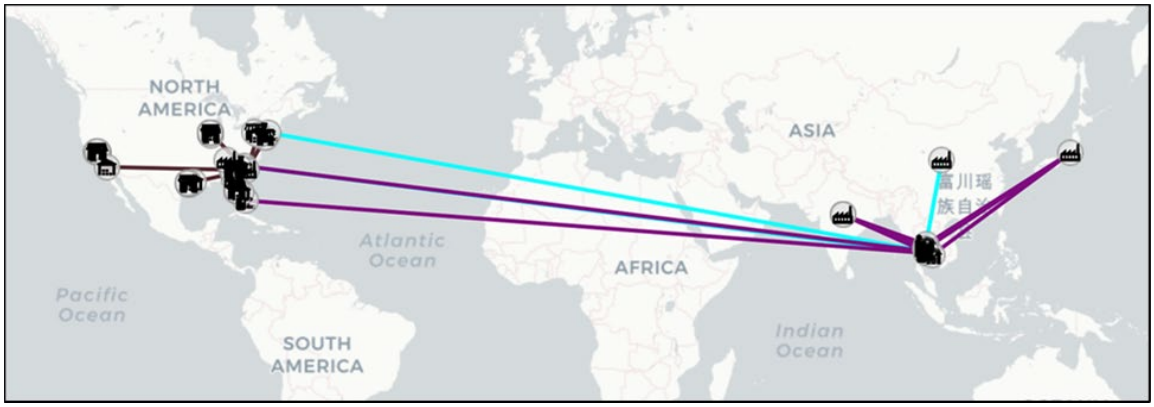

Figure 1: Shows production in Japan, China, India, and Thailand; with processing, distribution, and retail in the US.

The Teams

Red Team 1: Led by Brian Isle, this team assumed the persona of cyber criminals. They were focused on financial gain via ransomware by attacking an international multi-modal supply chain from source to consumer. The team was presented with a description of the supply chain and shown a graphical simulation as the food product moves through the supply chain. The team then brainstormed attack surfaces, speculated on vulnerabilities, and prioritized them.

Critical Assets

Multiple critical assets were identified by Team 1 but from the entire list. The top 5 were deemed to be most critical:

1. Executive/Administrative dept.
2. Processing Plant.
3. Seafood company email accounts.
4. Accounting Databases
5. Logistics company email accounts.

Attack Surfaces

Out of the many attack surfaces that existed, one was selected for each asset to be exploited. The attack surfaces are listed based on a score of 10 points awarded by each team member. Each of the top 5 attack surfaces align with the corresponding numerical marked asset.

1. Spearphishing directed at executives & management of companies.
2. Platform to attack email accounts and upload Ransomware.
3. Business Email Compromise (BEC) requesting financial documents from administrative staff.
4. Fake Credentials from former warehouse workers to use in a disinformation campaign.

Vulnerabilities

Narrowing down the list of associated vulnerabilities with corresponding attack surfaces, the top 3 were selected in decreasing order of critical vulnerability rating:

1. **Ransomware Platform:** Unpatched systems that exist within legacy services and systems offer the perfect target for malware embedded in emails.
2. **Business Email Compromise:** Requesting administrative financial documents ⇾ lack of any Domain-based Message Authentication, Reporting and Conformance (DMARC). Additionally, there is poor security awareness and staff training policies.
3. **Spear Phishing:** Directed to management ⇾ done via email targeting management spoofing new executive hires with an accompanying spreadsheet of macros. Open services is a prime vulnerability linked to this attack surface.

Attack Scenarios

Listed below are two possible attack scenarios that exploit the previously listed top vulnerabilities.

1. In the first scenario, job advertising emails can be sent to employees who are at risk of being terminated. These emails can contain links to the job site that contain malware that prey on vulnerabilities in Windows servers. This attack scenario corresponds to unpatched systems with legacy services and systems attack from embedded malware in emails.
2. This scenario utilizes four unique phishing campaigns that incorporate a combination of attached payloads and malicious links to access to the command and control server (C2). Special focus is given to blocks and dropped beacons.
    - Aims/Context/Perspective
    - Actions/Analysis.

Red Team 2: Led by Todd Carpenter, team 2 assumed the role of a malicious corporation with the goal of adulterating a food product as it passes through an international multi-modal supply chain from source to consumer. The team was presented with a description of the supply chain and shown a graphical simulation as the food product moves through the supply chain. The team then brainstormed supply chain attack surfaces, speculated on possible vulnerabilities that could be exploited, and prioritized the vulnerabilities based on the effectiveness of meeting the goal of damaging their competitor.

Critical Assets

A wide variety of assets at multiple stages of the chain were considered by the red team. But the following five were identified as the most valuable:

1. Processing: packaging plastics.
2. Processing: Warehouse cooling and freezing.
3. Container shipment worldwide.
4. Processing: packaging plastics.
5. Processing: Warehouse cooling and freezing.

Attack Surface

1. Ordering databases.
2. Ship control systems for engines.
3. Electronic shipping manifests.

Vulnerabilities

1. **Unpatched systems:** identified throughout the supply chain, allowing for standard pre-packaged attack tools to gain entry and make changes. Why worry about cracking passwords when you can waltz your way in through an open hole?
2. **Control systems:** Ship engines share the problem of being unpatched. Whilst also being vulnerable to attacks through the engine supplier, this could be achieved through spearfishing attacks or more direct targeting of the web interface for the management system used.
3. **Attracting other malign attention:** Publishing of information about vulnerabilities to encourage ransomware attacks to act as a distraction from the team's activities.
4. **Compromised employees:** These could provide a route into a number of attack surfaces across the supply chain. Workers who are about to be made redundant might be more likely to give up information.

Attack Scenario

Attack on shipping manifests. Red team 2 found that the first step in a successful attack on the manifest would be thorough reconnaissance of the systems used by distributors. Information about key individuals, the location of servers, and the versions of software used were all identified as useful tools for an attacker to have in their arsenal.

Once this information has been gathered, spear phishing attacks disguised as contact from recruitment firms, or workers unions could be utilized to compromise employees and gain admin access to the manifest system. From here, products could be shipped to the wrong location, starving some parts of the supply chain and causing bottlenecks in others, products stuck in port at customs would quickly spoil and quickly become unusable resulting in significant product losses.

After-Action Reflections on the Analytical Red Team Exercise

Brian Isle and Todd Carpenter led the two Analytical Red Teams through the analysis process. Todd and Brian have two decades each of team based analytical red teaming both as practitioners and instructors of the process. The following captures their observations on the exercise and analysis process.

Brian noted that his team was able to investigate the given scenario and quickly identify attack surfaces and vulnerabilities. Within the short timeframe, they only pinpointed one vulnerability for each attack surface. Nevertheless, the team found that the disgruntled former employees provide a salient opportunity for phishing attacks through unsecured emails. Businesses should note the 40-minute exercise provided enough time to generate a rich analysis of the supply chain vulnerabilities.

Todd reported that Team 2 considered a broad range of approaches, from adulterating packaging to targeting the shrimp itself by altering the quantities of antibiotics administered to attacks on HVAC systems. Given the length of the supply chain, and the imperative of refrigeration, a single interruption to cooling at any point along the supply chain would have significant effects. Thus, various points can be targeted and a different target can be selected for further attacks, making it difficult for them to guarantee the integrity of the supply chain (to "keep it in place"). Team 2 narrowed in on shipping manifests as a means to alter product orders, delivery timings, and delivery locations. To access these, the team considered multiple routes in, including SaaS platforms, phishing attacks on former employees, and communication channels to and from container ships.

Summary of the Analytical Red Team Process

The Analytical Red Team process provides a first step in the security process to develop an informed strategy and to direct security resources to the most needed areas. The process should be repeated periodically based on the organization security readiness. The seven-step process is described below.

The goal of the exercise was to show the analysis process, not to produce a complete analysis. Due to the limited available time of 35 minutes for the actual red-teaming, we pre-established the threat agents and their goals. We simplified the decision-making by using a simple vote, versus using more sophisticated decision metrics. Also due to time constraints, we did not attempt steps 6 and 7.

The premise of this analysis is to have the team think like the threat agent. Each red teamer is to adopt the goals and limitations of the threat agent. Limitations include both technical capability and cost to undertake the attack. Cost is measured in both financial terms and risk to the threat agent.

The Red Team works best with a diverse group of people, such as financial, technical, and business. These can be insiders who know the business, who may not be security experts, can make great Red Teamers.

The analysis provides insight into where an attack might occur (the most probable critical asset), possible attack surfaces at the location, probable vulnerabilities associated with the attack surface, and scenarios describing how the vulnerability might be exploited. With this information one can investigate the status of safeguards and security controls for each of the identified vulnerabilities.

Analytical Red Team process

The following is the seven step Analytical Red Team process.

1. Define the assessment goals and threat agent(s).
2. Identify critical assets of the assessment target.
3. Gather information on the critical asset to identify attack surfaces and vulnerabilities.
4. Develop attack scenarios that exploit vulnerabilities and attack surfaces.
5. Prioritize vulnerabilities / targets in the supply chain.
6. Identify shared vulnerabilities and common attack enablers.
7. Develop mitigation strategy.

Analytical Goals

Key qualities of a useful analysis process include: the process should self-document, produce repeatable results, enable comparison of results over time, and enable reuse of the analysis for subsequent reviews. For the exercise we used the seven-step analytical Red Team process that is discussed elsewhere in this report. The process has been applied broadly for two decades and found to be flexible, easy to use, and deliver meaningful results. It is consistent with national security standards such as NIST SP-800-30-r1). The participants in the exercise were quickly able to grasp the process and deliver meaningful results.

The analysis process should specify the decision-making approaches to use when following the process. The decision-making metrics should provide a scoring range and be easily understood by the team members. The metrics will improve communications between the team members, resulting in better decision making. Since the results will then be metrics based, it will make it easier to compare results as the process is re-applied over time, for example when either the threat or the system under study changes. For the exercise we applied a quick Pareto voting method where each team member placed five votes to indicate the attack features that they deemed were the most important.

The analysis process should self-document as the team proceeds through the process. Without such documentation, writing up results afterward based on faulty recollections can introduce inaccuracies, or biases from the person(s) performing the write-up. The method used to capture the results does not need to be complex nor onerous to use. For this exercise we used Google Sheets with a 4-page spreadsheet, with each page capturing a step in the process. The Google Sheets allowed the virtual team to enter their inputs in real time. The exercise participants were able to quickly become familiar with the Google Sheets and the architecture of the tool. (See tables 1 -4) Google Sheets has adequate security and access control for a public exercise. Security for a real assessment, however, should be considered ahead of time, and satisfy organization specific requirements.

Pleasant surprises

The objective of the analytical red team exercise was to show the process steps of the two teams analyzing a realistic international supply chain. The exercise was only 35 minutes long and it was believed that the results would be limited and at best notional. The team leads (Brian and Todd) were pleasantly surprised at the quality of the analysis and the results from the 35 minutes of work. The distributed team members came to the virtual table ready to discuss the critical assets, the potential vulnerabilities, and how to exploit the vulnerabilities. The results were meaningful and usable despite only addressing 4 of the 7 process steps in the brief time available. This quality of the results was particularly surprising because this was a fully virtual exercise with only a few of the team members personally knowing each other, and the first time using this particular distributed platform. By comparison, prior experiences performing similar analysis with a team of 6 to 8 people in face-to-face meetings usually took about ½ day to complete the same 4 steps.

Red Team members & expert feedback

For a process to stand the test of time it must engage the participants, produce real results that can be applied, and be a pleasant experience. These three requirements must be universal for all the team members. This is a tall order because the team members had a variety of backgrounds and were not all security experts. Based on the personal feedback that the team leads received after the exercise, we believe that we met the three requirements.

Richard Stiennon commented on his team's identification of ways to adulterate through supply chain disruption, rather than by direct adulteration only. The perishability of the goods allowed for any part of the supply chain involving refrigeration to be targeted and exploited.

Dr. Roxanne Everett, Cyber Strategy and Infrastructure Department Chair, College of Information and Cyberspace at the National Defense University, observed that team members could have drawn parallels with current supply chain issues we are facing due to the COVID-19 pandemic. For instance, cleaning product supply chain interruptions that are not attributable to malicious intent. In her analysis, examining natural shortages such as these can provide insights into how to "strike unobtrusively," either in terms of mimicking their effects or by otherwise masking attempts at adulteration. In some aspects, she thought they could have been "more deliberate and a lot more evil."

Table 1: Identify Critical Assets

Red Team 2: Malicious corporate competitors focused on adulterating the food supply chain

Step 2: Identify critical assets of the assessment target

Critical Assets	Todd	Justin	Richard	Wendy	Stephen	Amy
1	Packaging Plastics	Processing/Warehouse: Cooling/freezing	Container shipment worldwide	Processing : scheduling of production runs	Distribution: exporter manifest / inventory management system	
2	Production: fish meal, oil, antibiotics	Processing: MES/ERP/EDI/Recipe systems	Port authority (Customs and quarantine)	Processing : adjust "recipes" for production	Storage: "Smart" Refrigerated Shipping Containers ("Reefers")	
3	Processing: sizing	Farm: MES/ERP/EDI system	Store freezers	Warehouse : HVAC system, employee discomfort	Storage: holding warehouse environmental controls	
4	Processing: packaging	Processing: Processing lines	Processing: Hygiene (gloves, gowns, scrubbing)	Transport : refrigeration systems	Processing: processing line fryer	
5	Processing: freezing	Processing: Distribution	Fishing fleet weather system	Warehouse : common chillers with HVAC for refrigeration	Processing: processing line HMI	
6	Distribution: Importers / Exporters	Farm: Food/supplements	Truck fleet	Shipping dock : bills of lading for trucks	Processing: processing line (fryer) sensors	
7	Transportation: refrigeration	Port: Product storage	Container shipment worldwide	Shipping dock: coordination of orders	Processing: processing line historian	
8	Storage - warehouse - refrigeration	Port: Trucking	Store stocking systems	Farm : temperature controls	Shipping / Sales: orders processing system	
9	Processing: Inject Gelatin solutions	Port: Customs		Farm : incorrect supplement orders		
10		Farm: Water chemistry		Port : modify bills of lading for shipping		

Directions:

1. Identify what you believe are the critical assets in the supply chain relevant to your goal.
2. List your critical assets under your name.
3. After short discussion, prioritize and push your top three critical assets to the top of your list. These CA's will carry forward to step 3.

Definitions

A critical asset is an entity in the chain that if taken down would greatly hinder the flow through the supply chain – and – difficult to quickly replace.

Table 2: Gather Information on the Critical Asset to Identify Attack Surfaces

Red Team 2: Malicious corporate competitors focused on adulterating the food supply chain

Step 3A: Gather information on the critical asset to identify attack surfaces

			Vote for attack surface that is easest to exploit based OSINT						
	Top Critical Assets	**Attack Surfaces**	**Todd**	**Justin**	**Richard**	**Wendy**	**Stephen**	**Amy**	**Total**
1	Packaging Plastics	Logistics: ordering databases	1		1	1	1		4
		Networks: electronic orders & transmission							0
		Personnel: personnel records							0
		Personnel: email addresses, websites for recon							0
		Specifications: plastic requirements					1		1
2	Processing/Warehouse: Cooling/freezing	HVAC units	1	1	1				3
		Company and Vendor engineering and maintenance personnel							0
		Enterprise systems (pivot point)							0
		Industrial control systems			1	1			2
		Physical through in-person social engineering		1					1
3	Container shipment worldwide	AIS ship identity system							0
		Local GPS (spoofing)							0
		Ship control systems for engines (Remote mainatinance)	1		1	2			4
		Networks: electronic orders & transmission							0
		Crew staffing disruption			1				1
4	Processing : scheduling of production runs	MES system : automated scheduling		1		1			2
		Personnel : change operator schedules							0
		Equipment controls : individual machines							0
		Batch processing steps : change order, timing	1	1	1				3
		Historian							0
5	Distribution: exporter manifest / inventory management system	Exporter orders, inventory databases					2		2
		Electronic shipping manifests	1	1		1	2		5
		Email							0
		Employee ordering input workstation							0
									0
6		Specifications: formula							0
		Quality Control process							0
		Quantity - inject to bulk up even if not needed							0
		Farm suppliers							0
		Certifications of authenticity - mask the digital inspection results	1	1					2
			6	6	6	6	6		

Directions:
1. Brainstorm/discuss cyber/physical attack surfaces of the identified critical assets.
2. Document the attack surfaces.
3. Vote to select top Attack Surfaces. Five for votes each player.

Definitions:
1. The Attack Surface describes all of the different points where an attacker could get into a system, and where they could get data out.

Table 3: Identify Potential Vulnerabilities

Red Team 2: Malicious corporate competitors focused on adulterating the food supply chain

Step 3B: Gather information on the critical asset to identify vulnerabilities

				Vote for most likely vulnerability based in OSINT						
	Top Critical	**Attack Surfaces**	**Vulnerabilities associated with Attack Surfaces**	**Todd**	**Justin**	**Richard**	**Wendy**	**Stephen**	**Amy**	**Total**
1	Packaging Plastics	Logistics: ordering databases	Ancient unpatched systems	1	2		2			5
		Networks: electronic orders & transmission	unauthenticated							0
		Personnel: personnel records	Influence operations: bribe							0
		Personnel: email addresses, websites for recon	phishing, no authentication			1				1
		Specifications: plastic requirements	unencrypted, unsigned							0
2	Processing/Warehouse: Cooling/freezing	HVAC units	Unpatched, unauthenticated, Internet accessible	1		1				2
		Company and Vendor engineering and maintenance p	introduce/manipulate USB devices, physical access							0
		Enterprise systems (pivot point)	accessible systems							0
		Industrial control systems	Windows servers present, clear-text communications			1				1
		Physical through in-person social engineering	utilities (e.g. ammonia/glycol/power/etc.)							0
3	Container shipment worldwide	AIS ship identity system								0
		Local GPS (spoofing)								0
		Ship control systems for engines (Remote mainatinar	Engine supplier Windows 7, Satcom spoofing, onboard embedded windows vulns	1	1	1	2			5
		Networks: electronic orders & transmission								0
		Crew staffing disruption								0
4	Processing : scheduling of production runs	MES system : automated scheduling								0
		Personnel : change operator schedules	people moving, bitter because unemployeed. Knows secrets, so route into systems			1				1
		Equipment controls : individual machines								0
		Batch processing steps : change order, timing								0
		Historian								0
5	Distribution: exporter manifest / inventory management system	Exporter orders, inventory databases	unpatched vulnerabilities; unsecured remote access; compromised employee					3		3
		Electronic shipping manifests	unpatched vulnerabilities; unsecured remote access; compromised employee	1	3	1	2	3		10
		Email	BEC; phishing							0
		Employee ordering input workstation	unpatched vulnerabilities; unsecured remote access; compromised employee							0
		0								0
6		Specifications: formula								0
		Quality Control process	results stored in unpatched dB							0
		old process control								0
		operations network attached to business network								0
		Certifications of authenticity - mask the digital inspection results								0

Directions:
1. Brainstorm/discuss most likey vulnerabilities for top rated attacked surfaces.
2. Document the vulnerabilities.
3. Vote to select top vulnerabilities. Five for votes each player.

Table 4: Develop Attack Scenarios

Red Team 2: Malicious corporate competitors focused on adulterating the food supply chain

Step 4 & 5: Develop attack scenarios

	Top Critical Assets	Attack Surfaces	Vulnerabilities associated with Attack Surfaces	Scenarios to exploit top vulnerability	Vote for most likely scenario exploiting top vulnerabilities based in OSINT						
					Todd	Justin	Richard	Wendy	Stephen	Amy	Total
1	Packaging Plastics	Logistics: ordering databases	Ancient unpatched systems								0
		Networks: electronic orders & transmission	unauthenticated								0
		Personnel: personnel records	Influence operations: bribe								0
		Personnel: email addresses, websites for recon	phishing, no authentication								0
		Specifications: plastic requirements	unencrypted, unsigned	change specifications, e.g., thinner plastic, higher permeability							0
2	Processing/Warehouse: Cooling/freezing	HVAC units	Unpatched, unauthenticated, Internet accessible	Compromise Internet-accessible known vulnerability (or unprotected access) to pivot inside							0
		Company and Vendor engineering and maintenance personnel	Directed social engineering, unpatched OS/software, manipulated software, introduce/manipulate USB devices, physical access	Spear phishing, watering hole, USB drops							0
		Enterprise systems (pivot point)	Social engineering, unpatched OS/software, introduce/manipulate USB devices, externally accessible systems	Phishing, browser exploits, direct attacks on externally facing systems, USB drops							0
		Industrial control systems	Legacy devices, (little to) no authentication and authorization on ICS/OT devices, likely Windows servers present, clear-text communications	Modify set points, manipulate program/project files, gather and exfiltrate information, man in the middle attack to manipulate communications in-transit							0
		Physical through in-person social engineering	Physical manipulation/destruction/adulteration of refigeration and/or other dependent utilities (e.g., ammonia/glycol/power/etc.)	Sever critical connections, lock-out multiple locations, destroy different elements, release dangerous gases/liquids/solids into the environment							0
3	Container shipment worldwide	AIS ship identity system	0								0
		Local GPS (spoofing)	0								0
		Ship control systems for engines (Remote mainatinance)	Engine supplier Windows 7, Satcom spoofing, onboard embedded windows vulns								0
		Networks: electronic orders & transmission	0								0
		Crew staffing disruption	0								0
4	Processing : scheduling of production runs	MES system : automated scheduling	0	Create a mismatch between the orders and production, building up a backlog of products for which there is no deman							0
		Personnel : change operator schedules	people moving, bitter because unemployeed. Knows secrets, so route into systems	Digital schedules adjusted to bring "wrong" number of people to site, or wrong skillsets							0
		Equipment controls : individual machines	0								0
		Batch processing steps : change order, timing	0								0
		Historian	0								0
5	Distribution: exporter manifest / inventory management system	Exporter orders, inventory databases	unpatched vulnerabilities; unsecured remote access; compromised employee	Substitute adulterated shrimp (e.g., illegal antibiotic used; high salmonella count from contaminated growing pond; spoiled) from untrusted farmer for shrimp from trusted/vetted source.							0
		Electronic shipping manifests	unpatched vulnerabilities; unsecured remote access; compromised employee	REcon - find people, locations. What version of OS? Expoit: speare phishing especially disinfranchised employees. Also moving to SaaS to get connections to existing manifest root access for sysadmin - probe sys for vulns Update shipping manifests - move things wrong places, cause port entry issues. Mark real shipments with notices that require quarantine analysis send to port entry that can't handle allergins - peanuts and shellfish. If you send too much stuff into a location, you'll create a bottleneck. Stuffing part of the supply chain, starve other parts. Logistics attack.							0
		Email	BEC; phishing								0
		Employee ordering input workstation	unpatched vulnerabilities; unsecured remote access; compromised employee								0
		0	0								0
6		Specifications: formula	0								0
		Quality Control process	results stored in unpatched dB	inject filter to permit passing out-of-spec batches							0
		Quantity - inject to bulk up even if not needed	0								0
		Farm suppliers	0								0
		Certifications of authenticity - mask the digital inspection results	0								0

Directions:
1. Brainstorm/discuss possible scenarios that exploit the most likely vulnerability.
2. Document the attack scenarios using headline description.
3. Vote to select top scenarios. Five for votes each player.