



CHAPTER 17: SCM PRODUCT FRAUD AND COUNTERFEITING

3
4
5
6
7
8
9
10
11
12
13

One important supply chain disruption (SCD) is from the intentional disruption act of product fraud and intellectual property rights violations of product counterfeiting. A supply chain key risk is from supply chain disruptions (SCD). SCD's can be unintentional or intentional. This content was developed to start with a review of SCM best practices, present "what" is product fraud and counterfeiting, "how" to reduce the vulnerability and focus on prevention, then most important to provide guidance on "how much is enough" and then "how to start." The content expands to the implementation and management of this supply chain management best practice.

Note: Pre-publication version
– missing all citations

14 This content in this chapter began as a teaching supplement to the SCM303 course. It was
15 first publicly presented in an invited presentation in June 2021 at the MSU College of Business
16 Executive Education program on Procurement and Supply Chain Management. (Ref ScmExed
17 date) The program was first offered in YEAR and DETAIL. The program is well known to be
18 recurring even to provide a broad and deep update.

19 The content for the executive education and the presentation builds upon supply
20 management and supply chain management best practices. One of the best practices is supply
21 chain risk management.

22 It is important to understand the overall resource-allocation decision-making structure
23 before reviewing how an enterprise addresses product fraud and counterfeiting. Of course, all
24 product fraud and counterfeiting incidents are "bad," but how bad? Should every event trigger a
25 recall of all products? Should the FBI and US Customs be contacted for every event? To consider
26 the thoroughness of the recommended action, throughout this text, a basic question is: "if your
27 CFO had \$1 million to spend on one project, would this be the highest priority project?" A typical
28 response is, "I'm not the CFO, so only they can make that decision." That is understood, but if
29 your recommendation does not consider other factors, such as where this vulnerability fits into all
30 other enterprise-wide risks, then your proposal is only a statement that 'the sky is falling!'" No
31 one has a better understanding of the problem than you and your expert team. If your proposal
32 does not present how this risk compares to all other enterprise-wide risks, then you are expecting
33 the subject matter non-expert CFO to decide for you. Further, if you become aware of how this
34 risk compares to all other risks, you can prioritize your resource-allocation requests.

35 The first step in understanding how this risk fits into all other risks is to step back to
36 review the scope of the enterprise and the activities:

- 37 • An enterprise could be a company, a non-profit organization (NPO), a non-governmental
38 organization (NGO), or a government.
39 • The scope is for all types of supply chain-related activities, from manufacturing products
40 such as automobiles or food to managing services such as a bank or hotel... or a classroom
41 of students... or you are planning for a dinner at home.

42

43

44

45

46

47

This statement is an important consideration when implementing countermeasures and control systems. It is essential to understand that many counterfeiters are intelligent, motivated, creative, patient, persistent, and stealthy. While there are some low-tech/ low activity fraudsters, there are many that are very competent. Why wouldn't they attend public events about anti-counterfeiting? Do you conduct market research on your competitor? Of course. Would you be stealthy and attend a public meeting about the strategic direction of your competitors? Of course. While it is incredibly frustrating to realize that the "bad guys" will follow your every move, it is also helpful to move beyond the idea that your strategies will be confidential indefinitely. Of course, some information does stay confidential, but there is a shelf-life on secrets. In addition, some of the secrets may need to be revealed, such as when prosecuting a court case. To explain how you know a product is counterfeit, you may need to reveal a covert or overt anti-counterfeiting feature (e.g., lack of hologram, incorrect authentication code, lack of a microtaggant in the printing, an unauthorized ingredient in a product, etc.).

So, there are three key insights from this:

- 1) the counterfeiters monitor our activities and strategies
- 2) there is a shelf-life of secrets, and confidential strategies may become known
- 3) anti-counterfeiting systems may need to be revealed for the prosecution of a court case.

From these insights, there are three countermeasures:

- 1) If the counterfeiters are listening, let's use that communication channel to alert them there is a risk of attacking your product – they might get caught!
- 2) If the confidential countermeasures become known after 18 months, shift to a 12-month cycle for refreshing activities.
- 3) If the confidential countermeasure needs to be revealed in five court cases per year, use ten features.

Remember, the goal is not to catch product fraud and counterfeiting but to prevent it from occurring in the first place. While it is frustrating that counterfeiters are intelligent adversaries, there is a logic to accept that premise and embrace it. When we accept that reality, we can implement work processes that reduce the vulnerability of shifting product fraud and counterfeiting threats.

This chapter will set a foundation to understand that underlying fraud opportunity and consider the most efficient and effective countermeasures and control systems for your enterprise.

81 1.01 Defining Product Fraud including Counterfeiting

82 **Product fraud** is generally considered intentional deception for economic gain using
 83 material goods (see below for a full review of the standards and definitions). (REFs) This broad
 84 definition is consistent with many of the world's activities, including the International Standards
 85 Organization, the European Union, the United Kingdom agencies, the Chinese agencies, the
 86 Global Food Safety Initiative (GFSI), a range of private standards and certifications, and others. In
 87 the United States for food and drugs, a related term is "economically motivated adulteration" or
 88 EMA. The US FDA has a working definition of EMA as a "substance" for "economic gain," and
 89 their focus is only on public health threats.

90 The types of product fraud including: adulterant-substances (e.g., dilution, substitution,
 91 and contaminants), tampering of the documents or package, production over-run, theft,
 92 diversion, simulation, and intellectual property rights infringement counterfeiting (Table Error!
 93 **No text of specified style in document.-1**). (REF JFS1)

94
 95 **Table Error! No text of specified style in document.-1: Types of Product Fraud including definitions and food
 96 examples (REF BFF?)**

Term	Definition	Example
Adulteration (Adulterant-Substance)	A component of the finished product is fraudulent	Melamine added to milk
Tampering	Legitimate products and packaging are used in a fraudulent way	Changed expiry information, product up-labeling, etc.
Over-run	Legitimate product is made in excess of production agreements	Under-reporting of production
Theft	Legitimate product is stolen and passed off as legitimately procured	Stolen products are commingled with legitimate products.
Diversion	The sale or distribution of legitimate products outside of intended markets	Relief food redirected to markets where aid is not required
Simulation	An illegitimate product is designed to look like but not exactly copy the legitimate product	"Knock-offs" of popular foods not produced with same food safety assurances
Counterfeiting	Intellectual Property Rights infringement, which could include all aspects of the fraudulent product and packaging being fully replicated	Copies of popular foods not produced with same food safety assurances

97
 98 Product fraud can occur or enter the supply chain at any step and in any lane. First, a key
 99 is to broaden the lens to consider the entire supply chain, including outside the usual focus. The
 100 legitimate and authorized supply chain includes (1) inbound goods, (2) in manufacturing, and (3)
 101 finished goods. (REF X) For many products such as foods, most focus has been on inbound goods

102 and supplier quality assurance. This focus on ingredients is a natural extension of food safety best
 103 practices between the supplier and customer. There has been a high awareness of food fraud at this
 104 supply chain node, and there are clear responsibilities and actions for countermeasures. There is a
 105 great deal of focus on this transaction and quality control.

106 The next supply chain lane is (4) technology transfer & contract manufacturing. (REF)
 107 This lane is usually outside the responsibility of the supplier quality assurance function. An
 108 exception is that often the contract manufacturers are included as an inbound goods supplier.
 109 Usually, the agreements are initiated and managed by the legal function or another corporate
 110 group. The legal team would monitor the relationship's legal aspects, which may not include the
 111 same level of scrutiny and oversight for product safety and product fraud prevention. The legal
 112 agreements for technology transfer and contract manufacturing are often beyond the responsibility
 113 of the quality assurance team, so there usually needs to be an overarching corporate initiative to
 114 combine the activities. Finally, (5) outside the supply chain includes all counterfeit and fraudulent
 115 products in every way. This product was not created in the legitimate or authorized supply chain,
 116 so there was never any opportunity for oversight, tracking, or detection of the product. This lane
 117 is outside the supply chain, so beyond the control of traditional supplier quality assurance
 118 activities. The oversight often begins with corporate security function or other outward-facing
 119 market controls such as distributor monitoring.

120 /

121 Table Error! No text of specified style in document.-2: Where Product Fraud Occurs in the Supply Chain
 122 (REF)



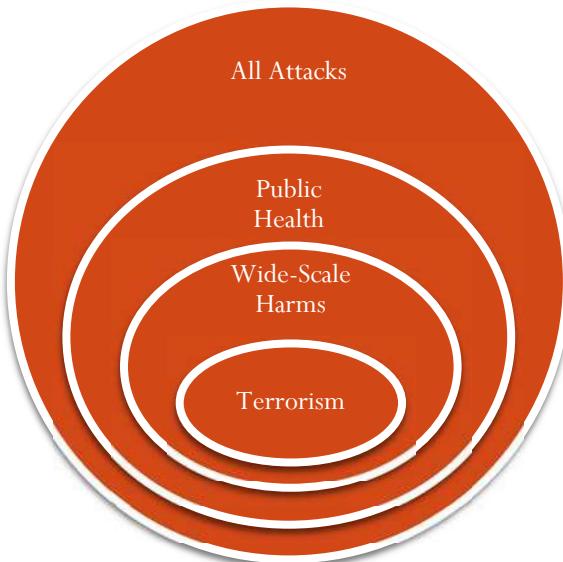
123

124 /

125 While management, monitoring, and control of all the supply chain lanes is complex and
 126 requires an interdisciplinary team, the enterprise must control all lanes to serve (6) the consumer
 127 when a retailer or consumer buys a product, and they expect it to be safe and genuine regardless
 128 of the method of purchase. If safety or fraud issues occur at any point in the supply chain, the
 129 product – YOUR product – could be recalled or deemed unfit for commerce. With this in mind,
 130 the industry standards such as for GFSI include the full scope of all types of fraud, for all types of
 131 products, and through all supply lanes. The “bad guys” could attempt any type of fraud against any
 132 type of product in any supply lane, so to reduce the fraud opportunity, your strategy must be
 133 inclusive of all.

134 The objective of the deception is the economic gain for the fraudsters. This detail requires
 135 a fundamentally different approach than for other product risks. For example, the goal of food
 136 fraud is for economic gain, while the goal for a food defense act is harm such as economic, public

137 health, or terror (for more on the food risks, see the food case study chapters). (REF) When
 138 mentioning food defense, it is important to emphasize further that there is a range of compliance
 139 requirements from the all-encompassing scope of the food standards, the public health harm focus
 140 of the US Food Safety Modernization Act (FSMA), and then the more narrow FSMA Intentional
 141 Adulteration Final Rule that only covers “wide-scale harm to public health,” and then attacks
 142 explicitly carried out by entities that meet the legal definition of a terrorist organization (Figure
 143 x). (REF, REF, REF)
 144 /



145
 146 **Figure Error! No text of specified style in document.-1: Hierarchy of Types of Food Defense Root Causes**
 147

148 The result of the fraud act is an economic or public health impact. There is always an
 149 economic threat for the industry or government. The industry is being cheated of a legitimate
 150 product sale, the risk to the brand value, or the increased costs for investigations and prosecutions.
 151 When there is a public health threat, then the governmental public health agencies are involved.
 152 For example, when illegally added melamine substance was found in infant formula and pet food,
 153 the US FDA quickly investigated and responded to the problem. When the current public health
 154 threat subsided and became more of an economic threat, public health agencies would turn the
 155 problem over to the criminal or commercial fraud agencies. To note, product fraud is often highly
 156 complex to investigate and prosecute compared to traditional actions against “drugs, guns, and
 157 violence.”

158 Also, the criminal enforcement agency does not have as much expertise in the complex
 159 and wide-ranging types of product fraud and criminal networks. Product fraud prevention falls
 160 into a unique category where expertise is needed from the public health agencies, and
 161 investigation expertise is required from criminal enforcement agencies. Also, it must be
 162 considered that while the economic threat is significant, it often falls very far down the law
 163 enforcement priority setting. (REF BFF, chapter) It is NOT that addressing product fraud is DE-
 164 prioritized; the resource runs out after being allocated to other higher priority problems.

165 Overall, with vastly constrained resources, this complex problem with a very low public
 166 health threat and a relatively low economic threat, holistically addressing product fraud prevention
 167 has not been mastered. But, while there may be a minimal or no public health threat, there is
 168 always a present vulnerability. The mishandling of the product, and lack of oversight of the good

169 manufacturing practices of the fraudsters, create a constant and evolving vulnerability. This
 170 inherent vulnerability is a root cause for enterprise-wide risks, including product safety. A
 171 proactive approach has led industries such as foods to expand current quality management systems
 172 to address product fraud (food fraud). For example, in 2002, the Consumer Goods Forum (an
 173 international group of products companies) created the Global Food Safety Initiative (GFSI) to
 174 coordinate common, industry-wide food safety prevention. With a focus on the root causes of
 175 food safety incidents, in 2017, the GFSI announced food fraud prevention standards that are now
 176 required within food safety management systems.

177 Several aspects of the food industry efforts for food fraud prevention are significant:

- 178 1) A standard definition and scope of food fraud are agreed upon.
- 179 2) There is a management system focus on prevention, not just detection or mitigation.
- 180 3) Addressing food fraud is a requirement in the common industry standard.
- 181 4) Together these enable harmonization and sharing of best practices.

182
 183 Defining product fraud and counterfeiting is a crucial starting point before addressing
 184 prevention.

185 186 1.02 Sidebar: Deceptive and Non-Deceptive Counterfeit 187 Products

188 There is a unique challenge for some anti-counterfeiting efforts where some consumers
 189 seek the fakes. There are categories of deceptive and non-deceptive counterfeits. (REF BFF)
 190 (OECD 2008; Spink 2017):

- 191 192 • **Deceptive Products (counterfeits):** products that are placed into supply chains with
 193 the intent to deceive the consumer into believing that the product is genuine in every
 194 way.
- 195 • **Non-deceptive Products (counterfeits):** products that do not position to deceive
 196 the consumer into believing the products are genuine by their positioning in the market,
 197 whether through the type of retail outlet in which they are sold (flea market, etc.), the
 198 price (exponentially low), or the quality (noticeably poor).

199 A further classification for the counterfeit product is by where the product is sold,
 200 including a primary and a secondary market. (REF BFF) (REF Spink 2017)

- 201 • **Primary market:** sales through authorized resellers which are for “Consumers who
 202 demand goods of genuine, non-infringing origin establish a market that is referred to in
 203 this report as the primary market (Spink 2019). For a fraudster to penetrate this market,
 204 to maintain the price and continued sales, the product must be able to deceive consumers
 205 into thinking they are buying genuine products (deceptive counterfeits)” (Spink 2019).
- 206 • **Secondary market** (possibly to the clearly illegal and clandestine black market): “Under
 207 certain conditions, consumers are often willing to purchase products they know are not
 208 legitimate” (Spink 2019). In this situation, the consumers usually understand something is
 209 not right or proper about the product, whether it is stolen, counterfeit, or otherwise
 210 substandard (non-deceptive counterfeits). “There are other markets in between such as

211 products not sold through authorized resellers, legal diverted product, or other types of
 212 ‘gray markets’’(Spink 2019).

213
 214 The non-deceptive counterfeits are often hard to combat since the consumers seek the
 215 fraudulent product. At the same time, there is less potential for brand equity damage due to
 216 inferior products since the customer knows the product is a fake. A key to reducing or controlling
 217 legal liability from counterfeit products' performance is to use anti-counterfeit features to identify
 218 genuine products. If there is a legal liability claim, the rights holder should clearly identify the
 219 difference between genuine and fake products. Often during an investigation or court case, a
 220 brand owner must provide that the branded product is a fake (see the notes above about anti-
 221 counterfeiting systems may need to be revealed publication in a court case.”).

222 There is often a misconception that the economic loss to a brand is not as simple as a 1-to-
 223 1 tradeoff for “removing one counterfeit product will lead to one more genuine product sale.”
 224 There is a hierarchy of “suitable replacements.”(REF USTR) This does apply to deceptive
 225 counterfeits where a customer may try to buy a discounted genuine replacement part (\$150), but
 226 a suitable replacement may be a generic product (\$200) that still costs less than a full-priced
 227 genuine product (\$500). This example is for non-deceptive counterfeit products.

- 228
- 229 • Hierarchy of suitable replacements for counterfeit products (based on the USTR example
 230 of luxury pants):
 - 231 ○ Luxury Brand “A” FAKE product: \$25
 - 232 ○ Luxury Brand “B” FAKE product: \$30 (if the consumer is seeking a very low price
 233 branded product but not exclusively “brand A.”)
 - 234 ○ Discount Brand “C” GENUINE product: \$30 (at the same price at brand “B,” the
 235 consumer may still choose the counterfeit.)
 - 236 ○ Midrange Brand “D” GENUINE product: \$60 (this may be above the maximum
 237 price point for the consumer, and if so, an acceptable alternative may be “no
 238 sale.”)
 - 239 ○ Premium Brand “B” GENUINE product: \$150
 - 240 ○ Luxury Brand “A” GENUINE product: \$200 (there may be a few consumers who,
 241 when they cannot find the \$50 fake product goes directly to buy the \$200 genuine
 242 product).

243
 244 In these scenarios, for deceptive or non-deceptive products, the value of reducing one (or
 245 1 million) counterfeit product sales is complex to estimate the increase in genuine product sales
 246 directly. With the “return” on reducing counterfeit products so unclear or undefined, it is
 247 inappropriate or impossible to use a direct and formal “return on investment” (ROI) formula. Of
 248 course, every expenditure of financial resources is expected to provide some value, but this does
 249 not necessarily meet the formal accounting principles of “investment” and “return.”(Ref acctg old
 250 ref, and Coso) This review explains why ROI is not the most efficient method to review product
 251 fraud prevention especially compared to using risk tolerance controls in COSO-based enterprise
 252 risk management (see the chapter on ERM and the case studies for food fraud prevention).

253
 254

255 1.03 Examples: Horsemeat in Beef including Hot Spot Analysis

256 Example: Horsemeat in Beef Across Europe in 2012 / Food Fraud Horsemeat 257 Incident review, supply chain mapping, and hot spot analysis

258 To review how and why product fraud occurs, it is helpful to (1) review an incident in
259 detail, including the fraud act, (2) supply chain mapping to track the fraud, and then (3) the
260 criminology hot spot analysis to identify the vulnerabilities that should be protected.

261 In 2012, a routine government import food inspection uncovered horsemeat illegally
262 added to the beef. (REF) Irish customs and food inspectors detected the incidents for products
263 coming from across Europe, with the two biggest sourced being companies in Poland and
264 Romania. (REF Taylor book, other) Once the findings were shared in official alters, horsemeat
265 was found in beef across the UK and Europe. The UK had the highest rate of incidence due to
266 several very active food brokers.

267 In some countries, horsemeat is produced under government regulations and legally sold
268 for human consumption. Often horsemeat is one of many species, or cuts of meats, that are less
269 expensive than beef. The price difference, combined with the oversupply of a species, creates a
270 fraud opportunity for illegal blending. In the horsemeat incident, horsemeat was blended into 50-
271 pound frozen blocks of bulk meat. The frozen blocks were frost-covered, so the product wasn't
272 easily inspected. Also, in many cases, the horsemeat was actually higher quality cuts of meat (more
273 muscle, less fiber, and other parts). No public health threats were found, so the typical food safety
274 detection would not have been engaged. The horsemeat/ beef products would have been labeled
275 correctly as higher quality in a meat quality test! A food quality test would not typically include a
276 species test at that time, so the horsemeat adulterant-substance went undetected.

277 Once the incident was made public, there was hysteria across the food industry and for
278 consumers. Food manufacturers and retailers began to test all beef products across their supply
279 chain urgently, including raw materials, in-process products, finished goods, and products in the
280 marketplace. Widespread recalls of products – whether proactive or based on test results – led to
281 bare store shelves. Consumers were both scared but seemingly even more outraged. In the UK,
282 horses are cherished pets and symbolic of childhood. The thought of eating a beloved pet was
283 outrageous.

284 Further, consumers started to question all their food and what other contaminants could
285 be hiding. This intense response did increase global awareness of the need for food fraud
286 prevention. Governments and industries took action. The UK funded the Elliott Review to
287 investigate the system weaknesses and recommend action. (REF Elliot) The EU started a Food
288 Fraud Network that coordinated activities between countries and with industry. (REF EU FFN)
289 The Global Food Safety Initiative (GFSI) shifted the direction of their already active GFSI Food
290 Fraud Think Tank from “what” is food fraud to “how” they could support prevention. (REF gfsi
291 fftt) Also, academia began shifting traditional food safety testing to food authenticity.

292
293 **Supply Chain Mapping for an Incident Review.** After identifying incidents, the
294 next step in product fraud prevention is supply chain mapping of the incident. Knowing the nodes
295 and links of the supply chain helps to point out the system weaknesses through criminology hot
296 spot analysis. This section will review the details of one of the sources of the horsemeat fraud
297 (Table Error! No text of specified style in document.-3 and Figure Error! No text of
298 specified style in document.-2). Remember, before this incident, species swapping was not a

299 significant concern in primary markets for large sales contracts. Also, in many situations, there is a
 300 low level of allowable “carry over” from making one product to another, such as shifting from
 301 producing pork sausage to beef sausage (There are exceptions where there is zero tolerance such as
 302 claims such as organic, halal, kosher, or for the major allergens.).

303 When the supply chain map is identified, there are three crucial insights. When it is
 304 presented in these simple steps, a significant vulnerability seems obvious.

- 305 1) The order and sale are an online system with only digital communication and no
 306 physical product management.
- 307 2) The product flow is between supply chain partners who have not interacted in this
 308 transaction.
- 309 3) There is an expectation that the product meets the specification as ordered, including
 310 the correct species as noted on the Certificate of Analysis and shipping information.
 311 To note, the typical receiving tests would be for food safety and quality level, not for
 312 species (at least not yet).

313
 314 **Supply Chain Mapping of the Incident.** The fraud act occurred when the meat
 315 producer deceptively and covertly co-mingled lower-priced horsemeat with beef (at node “7”).

316
 317 **Table** Error! No text of specified style in document.-3: Review of the Process Steps in the Horsemeat in Beef Fraud
 318 Transactions

#	Process
1	A headquarters of a food retailer (UK) “1” orders inventory replenishment of frozen lasagna from their manufacturing operations group “2” (France)
2	The manufacturing operations group “2” places finished product order with their procurement group “3” (Luxemburg)
3	The procurement group “3” opens up bidding, which receives interest from a series of brokers “4, 5, 6, 7, 8” (France)
4	The process ends with a broker “5” (Cyprus) who secures the contract with the buying group “3.”
5	The broker “5” sub-contracts with a logistics contractor “6” (Netherlands)
6	The logistics contactor “6” contract with meat producer “7” (Romania) to ship the product directly to the food retailer’s manufacturing operations “3” (the steps “4 to 8” never take possession or handle the product). Note: the meat producer “7” provides food safety pre-requisite program step of food authenticity confirmation and providing the Certificate of Analysis (CofA) = Product ships from the meat producer “7” to the food retailer’s manufacturing “3.”
7	The food retailer’s manufacturing operations “3” receives and produces the frozen lasagna before shipping to the food retailer’s warehouses (UK). Note: the CofA passes along the supply chain with the product. = Product ships to the food retailer “1” and into the UK market.

319 /

320 Next, the process steps are presented on a map (**Error! Reference source not**
 321 **found.**).

322



323
 324 **Figure Error! No text of specified style in document.-2: Geographic Map Depicting the Communication Enabling the**
 325 **Horsemeat in Beef Fraud (adapted from REF)**

326

327 **Criminology Hot Spot Analysis.** Now that the incident has been reviewed, including
 328 identifying the nodes and links, next is a review of the system weaknesses or vulnerabilities. From
 329 the step from “Crime Analysis for Problem Solvers in 60 Easy Steps”: (ref 60 steps)

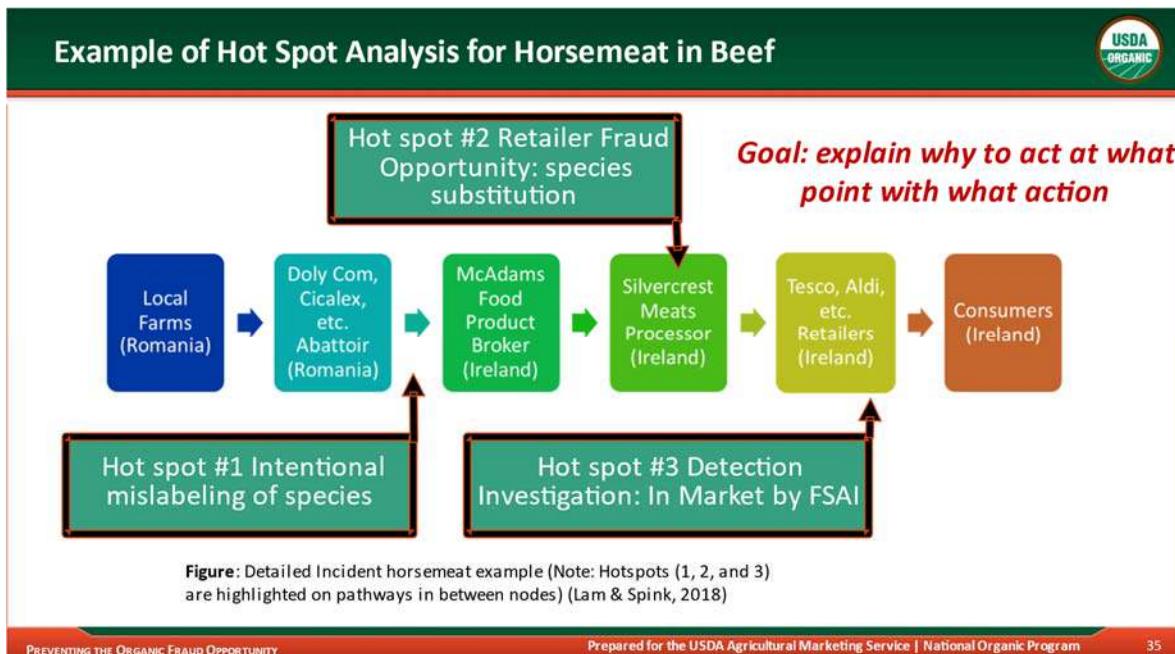
- 330 • **“Know how Hot Spots Develop”:** “To expand from just considering the geographical
 331 location and place where crime occurs, there is more insight to gain when considering
 332 three kinds of hotspots:”
- 333 ○ **Crime generators:** “places to which large numbers of people are attracted for
 334 reasons unrelated to criminal motivation. Providing large numbers of
 335 opportunities for offenders and targets to come together in time and place
 336 produces crime or disorder.”
 - 337 ○ **Crime attractors:** “places affording many criminal opportunities that are Well-
 338 known to offenders. People with criminal motivation are drawn to such locales.”
 - 339 ○ **Crime enablers:** “occur when there is little regulation of behavior at places:
 340 rules of conduct are absent or are not enforced.”

341

342 The goal of this activity is “why to act at what point with what action.” (REF usda2) Or,
 343 for a specific incident or types of incidents, to assess what specifically created the vulnerabilities, at
 344 what link or node in the supply chain did this occur, and then what unique countermeasure or
 345 control systems would reduce the system weakness). Using the horsemeat in the beef incident, the
 346 criminology hot spot analysis identified where the fraud act occurred (hot spot #1), where it was
 347 detected (hot spot #3) and then the most efficient and effective location to reduce the overall

348 system weakness (hot spot #2). Implementing investigative or confirmatory species tests at the
 349 processor is the most effective hot spot because this is a single pinch point in the supply chain.
 350 Also, there is the most control of the transactions because this is where the product is exchanged
 351 and can be inspected before payment. Also, consequences are effective and efficient since the
 352 buyer has possession of the product, and fraud identification would lead to notifying the
 353 government inspectors, including probably seizure and destruction of the products. The fraudster
 354 would risk 100% of their product for attempting a fraud act of 5 to 10% economic gain.

355 /



356
 357 PREVENTING THE ORGANIC FRAUD OPPORTUNITY
 358 Figure Error! No text of specified style in document.-3: Example of Hot Spot Analysis for Horsemeat in Beef -
 359 - from the USDA National Organic Program Training Course on Preventing the Organic Fraud Opportunity
 360 (Copyright use approved) (ref USDA citing Lam & Spink, 2018)

361 Supply chain mapping is crucial to identify vulnerabilities, and then criminology hot spot
 362 analysis helps to identify specific problem notes or links and then to help with the selection of
 363 countermeasures and control systems.

364 365 1.04 More About Standards and Definitions: ISO and COSO

366 The prevention management systems for product fraud and counterfeiting may be new for
 367 the supply chain management and the food industry, but there are international standards to build
 368 upon. There are supporting ISO standards that create a foundation:

- 369 • ISO 22380 Product Fraud: Product fraud countermeasures and control
- 370 • ISO 12931 Performance criteria for authentication to combat counterfeiting of material
 371 goods
- 372 • ISO 9000 Quality Management
- 373 • ISO 31000 Risk Management
- 374 • ISO 27000 Information Technology Security

- 375 • ISO 28000 Supply Chain Security
 376 • **COSO/ Enterprise Risk Management**

377
 378 The ISO standards include definitions. The first covers all product fraud.

- 379 • Reference: ISO 22380 Principles for Product Fraud Risk and Countermeasures:
 380 ○ Product Fraud (ISO TC292/ ISO 22380): Summary: deception utilizing material
 381 goods for economic gain or avoiding a loss;
 382 ■ “Wrongful or criminal deception utilizing material goods for financial or
 383 personal gain, Note 1 to entry: Fraud means wrongful or criminal
 384 deception intended to result in financial or personal gain creating social
 385 or economic harm, Note 2 to entry: Products include electronic media
 386 carried on material goods, Note 3 to entry: Fraud related to digitally
 387 transmitted electronic media needs to be considered separately.”
 388 (ISO/DIS 22380)
 389 ○ Prevention (ISO 22380): measures that enable an organization (3.158) to avoid,
 390 preclude or limit the impact (3.107) of an undesirable event (3.268) or potential
 391 disruption (3.70)
 392 ○ Protection (ISO 22380): measures that safeguard and enable an organization
 393 (3.158) to reduce the impact (3.107) of a potential disruption (3.70)
 394 ○ Disruption (ISO 22380): event (3.82), whether anticipated (e.g., a labour strike
 395 or hurricane) or unanticipated (e.g., a blackout or earthquake) that causes an
 396 unplanned, negative deviation from the expected delivery of products or services
 397 (3.181) according to an organization’s (3.158) objectives (3.153)

398
 399 The following ISO standard covers supply chain security:

- 400 • Reference: ISO 28000 Supply Chain Security
 401 ○ “...which shall include a) physical failure threats and risks, such as functional
 402 failure, incidental damage, malicious damage or terrorist or criminal action;”
 403 ○ Product Integrity (ISO 28002:2011),
 404 ■ “Property of safeguarding the accuracy and completeness of assets”
 405 ■ “The property of the unimpaired condition of the authentication element,
 406 the associated data, the information or the elements and the means for
 407 processing them” (ISO 28002:2011)
 408 ○ Security (ISO 28004): resistance to intentional, unauthorized act(s) designed to
 409 cause harm or damage to or by the supply chain
 410 ○ Security management (ISO 28004): systematic and coordinated activities and
 411 practices through which an organization optimally manages its risks and the
 412 associated potential threats and impacts there from
- 413
 414 • Reference: ISO 12931 Performance criteria for authentication solutions used to
 415 combat counterfeiting of material goods
 416 ○ Fraud:
 417 ■ ‘1) wrongful or criminal deception intended to result in a financial or
 418 personal gain

- 419 ■ ‘2) A willful act of deception that creates human or economic harm.
- 420 ■ Note 1 – types of fraud may include: product-related such as
- 421 counterfeiting, illicit diversion, alteration, intellectual property
- 422 infringement; Identity fraud such as identity theft (imposter fraud,
- 423 disguise, credential alteration) and document fraud such as cheque fraud,
- 424 banknote fraud, certificate fraud
- 425 ■ Note 2 – the consequences of “harm” and “deception” may vary between
- 426 jurisdictions and cultures.”
- 427 ○ Fraud opportunity: The conditions which provide an attractive target for
- 428 fraudsters, regardless of if a fraud has been perpetrated. This is similar to the
- 429 criminology concept of the “crime opportunity” in the “Crime Triangle.”
- 430 ■ Note1 – A crime triangle means three elements; 1. Motivated offender,
- 431 2. Suitable crime target, 3. The absence of a capable guardian.”

432 The awareness and reference to international standards help build a common language and
433 methods. The harmonization will enable the sharing of best practices.

436 1.05 Criminology and Crime Prevention

437 There are common criminology and crime prevention theories that apply directly to
438 product fraud and counterfeiting prevention. While it is crucial to emphasize enforcement and
439 prosecution, the most efficient activities are prevention that reduces the vulnerabilities. Product
440 fraud and counterfeiting are a hybrid type of crime with attributes of traditional crime (a physical
441 alteration between an adversary and a victim) and white-collar crime (distance in space or time
442 between the adversary and the victim). (REF WCC) What's even more challenging for
443 enforcement and prosecution is that the most common types of fraud are a hybrid – the methods
444 to address traditional crime or white-collar crime often need to be adapted and modified.

445 Further, beyond the fact that the adversary can be acting halfway around the world and a
446 month before the victim is defrauded, the types of fraud schemes often adapt to the unique and
447 often one-off fraud opportunities. No two fraud schemes are exactly the same. Thus, while it is
448 important to pursue enforcement and prosecution, the most efficient action is prevention.

449 The three focus areas are detection, deterrence, and prevention. (REF Spink et al. 2016a,
450 b):

- 451 ● “**Detection (detect):** is finding a specific adulterant-substance or product
452 anomaly.”
- 453 ● “**Deterrence (deter):** is a targeted countermeasure to stop one specific type of
454 food fraud or fraudster.”
- 455 ● “**Prevention (prevent):** is the application of countermeasures that reduce the
456 fraud opportunity.”

457 Fortunately, there is a criminology theory of Situational Crime Prevention that efficiently
458 applies to product fraud prevention. Situational Crime Prevention (SCP) is <history>. (REF)
459 (REF Clarke 1997) SCP is not a new science, but it is usually a new idea to apply to product fraud
460 prevention management. (REF Spink, Moyer, Park & Heinonen, 2013; 2014)

- 461 ● Four Components of Situational Crime Prevention: (REF Clarke 1997)

- A theoretical foundation drawing principally upon routine activity and rational choice approaches,
- a standard methodology based on the action research paradigm,
- a set of opportunity-reducing techniques, and
- a body of evaluated practice including studies of (crime) displacement.

Situational crime prevention comprises of opportunity-reducing measures that: (REF Clarke 1997)

- are directed at highly specific forms of crime,
- involve management, design, or manipulation of the immediate environment in as systematic and permanent way as possible,
- make crime more difficult or risky, or less rewarding and excusable as judged by a wide range of offenders.

Now that there is an underlying theory for applying crime prevention, it is important to review the types of counterfeiters.

- Types of Counterfeiter (REF Spink, Moyer, Park & Heinonen, 2013; 2014)
 - Recreational
 - Opportunistic
 - Occupational (Employee)
 - Professional

The application of Situational Crime Prevention can be visualized in the Crime Triangle. (REF CIEL?) The area of the triangle represents the crime opportunity or, for our application, the fraud opportunity. The goal of crime prevention is to reduce the crime opportunity. The crime opportunity is reduced by addressing one or more of the legs of the triangle, which are the factors of the victim, the fraudster, and the guardian and hurdle gaps.



Figure Error! No text of specified style in document.-4: The Crime Triangle that Visualizes Situational Crime Prevention (REF JFS1, types1, types2, WCC)

Since the adversary is a human, the most efficient scholarly field to engage in is social science, specifically criminology. The criminology theory of Situational Crime Prevention provides methods for reducing the product fraud opportunity.

497

498 1.06 Sidebar: Are you a habitual law breaker? Or, how to deter 499 Al Capone.

500 A simple exercise demonstrates how easy it is for humans to justify breaking rules (or
 501 laws) based on social norms. This even applies to humans that are not a criminal (not concerned
 502 with breaking the laws) or a sociopath (not concerned with cheating other humans). This has been
 503 used as a simple way to “think like a criminal.” As with many jokes or analogies, they do not
 504 translate everywhere, but this is usually effective overall.

- 505 • Question: how much over the speed limit do you drive on the highway? (ref BFF)

506 When I present this question, frequent responses are:

- 507 • Answer:

- 508 ○ *“But I’ve never been arrested or issued a speeding ticket citation.”*
- 509 ○ *“I’ve never been in an accident.”*
- 510 ○ *“If the road is icy, then I slow down.”*
- 511 ○ *“Oh, but under 10 miles per hour over the speed limit isn’t wrong.”*
- 512 ○ *“Everybody drives over the speed limit.”*

513 At this point, the justification often changes to rationalization such as “well, driving over
 514 the speed limit isn’t like making counterfeit medicines or producing knockoff luxury handbags.”

515

516 Considering these justifications, where does the actual legal speed limit fit into the
 517 consideration? If you drive over the speed limit, you are breaking the law. Period. You justify your
 518 activity, possibly because you’ve never been penalized. You know that some people have been
 519 caught since you’ve occasionally seen cars pulled over by the side of the road. You do occasionally
 520 see speed traps or traffic police monitoring by the side of the road. But you think those are really
 521 for the people who are drivers very, very fast and dangerous. Ah, here is a crucial point – a
 522 rationalization for acceptance that the infringement is ok. In part, the constant law infringement is
 523 ok since there are little or no penalties for driving less than 10 miles over the speed limit.

524

A couple more questions to consider:

- 525 • Question: If you are going to drive later today or tomorrow, what is the percentage
 526 chance that you will drive over the speed limit (knowingly and without remorse to
 527 break the law)?
- 528 • Question: If you do speed on a regular basis or basically constantly? Do you consider
 529 yourself unethical or immoral? Do you consider yourself a criminal? Why not?

530 So, back to the question about speeding. If society felt that driving over the speed limit
 531 was unacceptable for whatever reason, what would lead to near 100% compliance?

532

533 So now, considering this, how much over the speed limit would you drive? What if with
 534 the same level of resources (traffic police, prosecutors, tow-trucks, impound parking lots, and the
 535 societal support for the enforcement), that starting is six months, the penalty for driving 1 mile
 536 per hour over the speed limit was that your car was immediately impounded for one week, with
 537 you required to go with your vehicle, and a \$5,000 fine towing and retrieval. With this level of
 538 penalty, regardless of the level of enforcement, I bet you’d reset your regular habits long before
 539 the compliance date in six months. BUT, if after the enforcement started, you saw someone speed

540 by a state trooper (or you accidentally came over a hill and passed through a speed trap at 5 miles
541 over the limit), you might start inching your average speed back up. On the other hand, if you –
542 or someone you knew – experienced the penalty, you might just decide it's too risky to speed,
543 and you now always drive under (or well under) the posted speed limit. So, regardless of the level
544 of enforcement, the intensity of the penalty may dissuade you from driving over the speed limit. If
545 there is enough enforcement to remind you that some people are caught, the severe penalties
546 could lead to near 100% compliance.

547 To get back to the point of this example, a non-criminal and non-sociopath may feel it is
548 ok to counterfeit products (let's assume that the counterfeiters do not think that the products are
549 physically dangerous). Let's apply the same justification or rationalization from the speeding
550 example.

551 So, when considering the scope of product fraud prevention, it is most efficient to take
552 morals and ethics out of consideration since the worst case is we are dealing with criminals not
553 concerned with breaking the law, sociopaths not concerned about cheating others, fraudsters who
554 are often ignorant of the physical dangers of the products they produce, and habitual law-breaking
555 that is justified or rationalized. In general, a starting point in a product fraud prevention strategy is
556 to reduce the vulnerability or fraud opportunity. If there is no fraud opportunity, then there is no
557 fraud opportunity. Your supplier could be the notorious Chicago organized crime gangster Al
558 Capone, and he wouldn't commit fraud against you since there just isn't an opportunity. This
559 demonstrates how ordinary humans can justify habitually breaking the law and how reducing
560 vulnerability is the most efficient countermeasure.
561

562 **1.07 Applying Supply Chain Risk Management & Supply 563 Chain Disruptions**

564 The concepts covered in the previous chapter in supply chain risk management and supply
565 chain disruption have a unique application to product fraud and counterfeiting. A simple visual
566 way to understand the tradeoffs is to use the “Fundamental Supply Chain Process” triangle (Figure
567 Error! No text of specified style in document.-5). The ideal state is a balance of TCO total
568 cost of ownership, TPE total product experience, and Risk or variability that considers “what
569 could go wrong?” The optimal state is a balance that maximizes the unique goals of the
570 stakeholders. Every company has different characteristics of owner expectations, assets and brand
571 value, and customer expectations.
572

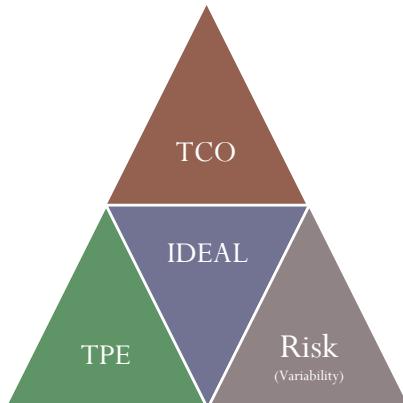
573
574
575

Figure Error! No text of specified style in document.-5: Fundamental Supply Chain Process" triangle (REF?)

576
577

When considering the supply chain management basics, it is important to start with the most basic definitions:

578
579
580
581
582
583
584

- **Supply Chain Risk:** “the likelihood and impact of unexpected macro and/or micro-level events or conditions that adversely influence any part of a supply chain leading to operational, tactical, or strategic level failures or irregularities.” (RefC)
- **Supply Chain Disruption:** ‘unplanned and unanticipated (event) that disrupts the normal flow of goods and materials within a supply chain.’ [(RefB) citing (Craighead et al., 2007)]

585
586

<Supply chain disruption section not included in this version>

587
588
589
590
591

Together, competent supply chain risk management includes consideration of supply chain disruptions. The disruptions are based on events that have causes of disruptions that produce an effect that has an impact on supply chain management. To achieve an optimal state, there is a balance of the TCO, TPE, and an optimal level of risk.

592

1.08 Applying Enterprise Risk Management/ COSO

593
594

<Not included in this version>

595

1.09 Call to Action for Product Fraud Prevention

596
597
598
599
600
601
602
603

Product fraud and counterfeiting is a problem that has often not been addressed from the perspective of a holistic and all-encompassing management system. When first reading this chapter, the process may seem overwhelming and impossibly complex to implement. Fortunately, there are many resources, guidance, training, and simplified steps. The bottom line is that product fraud and counterfeiting are a risk to the entire business. This is a risk that must be assessed to comply with a wide range of requirements such as food laws or financial reporting. You are addressing all risks that impact your work area is a requirement of being a company leader and competent manager.

604
605

Most basically, consider that the basic overall corporate compliance expectations for you to manage your business are:

- 606 • Have a plan
 607 • Confirm you follow the plan
 608 • Review and update the plan
 609

610 A starting point is a simple plan:

- 611 • Define your specific compliance requirements (SARBOX, FSMA, GFSI, etc.)
- 612 • Identify actual incidents or know the vulnerabilities
- 613 • Gather insight and guidance on how to start and how much is enough (such as reading this chapter and watching the supplemental video lecture)
- 614 • Seek training on the overview and details BEFORE starting assessments (for foods, review the free Food Fraud MOOCs, SSAFE training videos, etc.)
- 615 • Find a plan to meet the requirement
 - 616 ○ Gather incidents and vulnerabilities
 - 617 ○ Complete a vulnerability assessment
 - 618 ○ Develop and implement a prevention strategy
 - 619 ○ Create a plan to update and manage (not necessarily to keep doing MORE... maybe you have countermeasures and controls in place and could actually justify doing LESS)

620 To conclude with “Three Key Take Away Points”:

- 621 • Essential supply management and supply chain management include supply chain risk management (SCRM)
- 622 • Thorough SCRM includes a product fraud vulnerability assessment
- 623 • A VA is not that hard to start, and you are not going it alone

624 References

- 625 5. Porter, Michael E, *Competitive advantage: creating and sustaining superior performance*. 1985. 1985: New York: Free Press.
- 626 13. Swink, Morgan, Steven A Melnyk, Janet L Hartley, and M Bixby Cooper, *Managing operations across the supply chain*. 4th ed. 2020: McGraw-Hill Education New York, NY.
- 627 14. Johnson, P Fraser, *Purchasing and supply management*. Sixteenth ed. 2020: McGraw-Hill Higher Education.
- 628 15. Foster, S. Thomas, *Towards an understanding of supply chain quality management*. Journal of Operations Management, 2008. **26**(4): p. 461-467.
- 629 16. ISO, International Organization for Standardization, *ISO 9000: 2015 Quality management systems -- Fundamentals and vocabulary*, International Standards Organization (ISO), URL: <https://www.iso.org/standard/45481.html>. 2015.
- 630 17. ISO, International Organization for Standardization, *ISO 22380:2018 Security and resilience -- Authenticity, integrity and trust for products and documents -- General principles for product fraud risk and countermeasures*, Status: Published, Publication date: 2018-08-22 URL: <https://www.iso.org/standard/73857.html>. 2018.
- 631 18. Spink, John, Douglas C. Moyer, Hyeonho Park, and Justin A Heinonen, *Development of a Counterfeit Incident Clustering Tool (PCICT)*. Crime Science, 2014. **3**(3): p. 1-8.
- 632 19. Yeung, Andy C. L., *Strategic supply management, quality initiatives, and organizational performance*. Journal of Operations Management, 2008. **26**(4): p. 490-502.
- 633 20. Spink, John, *Food Fraud Prevention*. First ed. Food Safety and Microbiology. 2019, New York: Springer-Verlag. 686.
- 634 21. Schroeder, Roger G., Kevin Linderman, Charles Liedtke, and Adrian S. Choo, *Six Sigma: Definition and underlying theory*. Journal of Operations Management, 2008. **26**(4): p. 536-554.

- 652 22. Evans, James R and William M Lindsay, *An introduction to Six Sigma and process improvement*. 2014: Cengage
 653 Learning.
- 654 23. ISO, International Organization for Standardization, *ISO 31000:2009 Risk Management - Principles and*
 655 *Guidelines*. 2009.
- 656 24. Moore, David S, George P McCabe, Layth C Alwan, Bruce A Craig, and William M Duckworth, *The practice*
 657 *of statistics for business and economics*. 2016: WH Freeman.
- 658 25. ISO, International Organization for Standardization. *ISO 22000 Food safety management systems -- Requirements*
 659 *for any organization in the food chain*. 2005 [cited 2012; Available from:
 660 http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=35466.
- 661 26. ISO, International Organization for Standardization, *ISO 31000:2018 Risk management -- Guidelines*, URL:
 662 <https://www.iso.org/standard/65694.html>, 2018.
- 663 27. ISO, International Organization for Standardization. *ISO 28000 - Specification for security management systems for*
 664 *the supply chain*. 2007 [cited 2012; Available from:
 665 http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=44641.
- 666 28. ISO, International Organization for Standardization, *ISO 16678:2014 Guidelines for interoperable object*
 667 *identification and related authentication systems to deter counterfeiting and illicit trade*, URL:
 668 <https://www.iso.org/standard/57391.html?browse=tc>. 2014.
- 669 29. ISO, International Standards Organization. *ISO 12931 - Performance criteria for authentication solutions for anti-*
 670 *counterfeiting in the field of material goods*. 2011 [cited 2012; Available from:
 671 http://www.iso.org/iso/catalogue_detail.htm?csnumber=52210.
- 672 30. Ho, William, Tian Zheng, Hakan Yildiz, and Srinivas Talluri, *Supply chain risk management: a literature review*.
 673 International Journal of Production Research, 2015. **53**(16): p. 5031-5069.
- 674 31. DuHadway, Scott, Steven Carnovale, and Benjamin Hazen, *Understanding risk management for intentional supply*
 675 *chain disruptions: risk detection, risk mitigation, and risk recovery*. Annals of Operations Research, 2019. **283**(1): p.
 676 179-198.
- 677 32. Simchi-Levi, David, William Schmidt, and W. E. I. Yehua, *FROM SUPERSTORMS TO FACTORY FIRES*.
 678 Harvard Business Review, 2014. **92**(1/2): p. 96-101.
- 679 33. Macdonald, John R, Christopher W Zobel, Steven A Melnyk, and Stanley E Griffis, *Supply chain risk and*
 680 *resilience: theory building through structured experiments and simulation*. International Journal of Production
 681 Research, 2018. **56**(12): p. 4337-4355.
- 682 34. Craighead, Christopher W., Jennifer Blackhurst, M. Johnny Rungtusanatham, and Robert B. Handfield, *The*
 683 *Severity of Supply Chain Disruptions: Design Characteristics and Mitigation Capabilities*. Decision Sciences, 2007.
 684 **38**(1): p. 131-156.
- 685 35. Blackhurst, Jennifer, Christopher W Craighead, Debra Elkins, and Robert B Handfield, *An empirically derived*
 686 *agenda of critical research issues for managing supply-chain disruptions*. International journal of production research,
 687 2005. **43**(19): p. 4067-4081.
- 688 36. Melnyk, Steven A, DJ Closs, SE Griffis, CW Zobel, and JR Macdonald, *Understanding supply chain resilience*.
 689 Supply Chain Management Review, 2014. **18**(1): p. 34-41.
- 690 37. Speier, Cheri, Judith M. Whipple, David J. Closs, and M. Douglas Voss, *Global supply chain design*
 691 *considerations: Mitigating product safety and security risks*. Journal of Operations Management, 2011. **29**(7-8): p.
 692 721-736.
- 693 38. ISO, International Organization for Standardization, *Committee Draft of ISO/IEC Guide 73 "Risk management -*
 694 *Vocabulary"*. 2007.
- 695 /END/