Chapter 16
Risk Analysis (Part 2 of 3): Application to Food Fraud

Summary ***This chapter presents*** the risk analysis application to food fraud prevention. The risk analysis concepts and theories are well known and widely researched but not often adapted to the unique fraud opportunity and resource-allocation decision-making needs for food fraud prevention.

The Key Learning Objectives of this chapter are
- (1) **Risk Analysis:** Application of risk analysis to food fraud prevention
- (2) **Data Analytics and Big Data**: Introduction to data analytics and Big Data
- (3) **Extreme Events:** A review of extreme events, the highly improbable, and Black Swan events

On the Food Fraud Prevention Cycle (FFPC), this chapter addresses the "(0) fundamental concepts" beyond what is risk analysis to the details of risk assessment as applied to food fraud prevention (Fig. 16.1).

Introduction

This chapter continues the risk analysis topic on the application to food fraud. While the basic concept (risk is bad and something that should be controlled) and a method to judge the seriousness of a problem (likelihood and consequence) is clear, there is often little direction on actually applying the findings to a resource-allocation decision. To define a need to do "more," without a calibration with all other risks or resource-allocation options, is not usually helpful. There is value in considering the application to a specific problem which here is food fraud. When the project moves toward an actual decision, there are often questions about the data and data set. While risk theories are often not fully applied to a specific problem, the specification of the data and data sets is often not defined until questioned near the end of the process. It is helpful to understand the attributes of the data you have for your

J. W. Spink, *Food Fraud Prevention*, Food Microbiology and Food Safety,
https://doi.org/10.1007/978-1-4939-9621-6_16

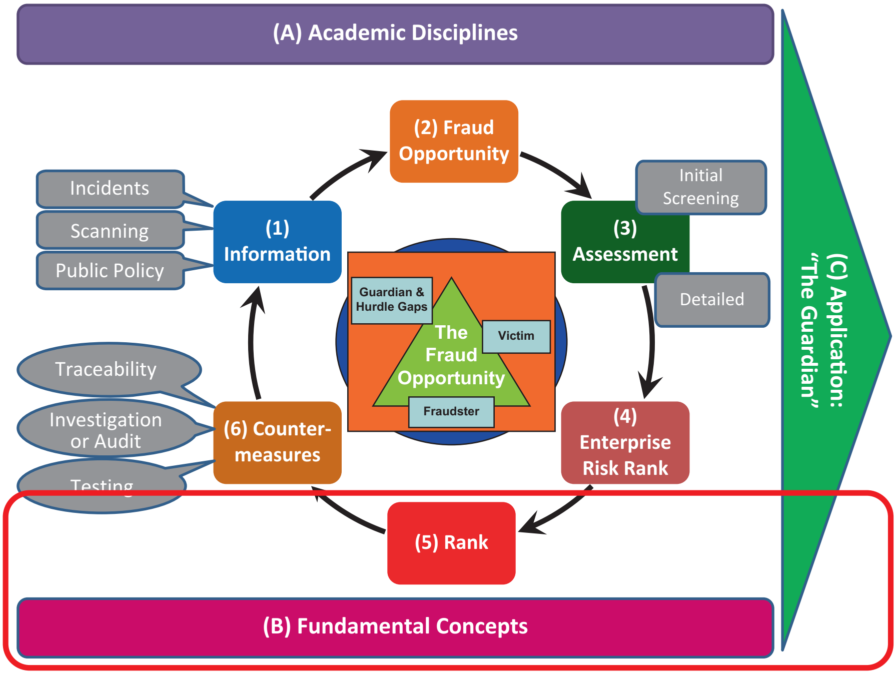


Fig. 16.1 Food Fraud Prevention Cycle—where this chapter applies to the overall concept: "(B) fundamental concepts" and "(5) risk" (Copyright Permission Granted) (Spink 2014; Spink et al. 2019)

review. When the analysis of a risk moves through an assessment and consideration of countermeasures and control systems, there is sometimes an awareness that all of this formality is based on some very extreme and improbable events…and can they even be predicted or prevented? These are sometimes referred to as Black Swan events. Fortunately, as with other parts of food fraud prevention, there is already a well thought through and thoroughly researched body of scholarship to draw upon.

Key Learning Objective 1: Application to Food Fraud Prevention

This section reviews the application of food fraud prevention in terms of how the assessment is presented. The presentation focus here is on the format of the finding.

The Key Learning Objectives of this section are

- (1) Review the insinuations made from an assessment including accuracy, precision, and certainty.

- (2) An overview of the definitions of the types of risks from across many disciplines to make sure to be clear in risk communication.
- (3) Then consider the nature of the data set and risk management needs to understand the most efficient format for presentation of the data and recommendation. The presentation format questions include qualitative or quantitative, also words or numbers, the amount of analysis required for the decision at hand, and others.

Appropriate Precision, Accuracy, Certainty, and Presentation of Findings

Albert Einstein is reported to have said: "everything can be counted, but not everything counts." This applies to food fraud prevention both in the evaluation of the underlying data sets and the subsequent assessments. Judgments of the source and type of information (e.g., raw data, information, and then more advanced and formally defined intelligence) are covered in more detail in the Criminology chapter. A series of incidents are provided that contribute to very important insights into the fraud opportunity, and the final reports should take into consideration the nature of the underlying data. For example, a wide range of statements of the economic impact of counterfeiting and piracy are presented with high-level statistical analysis but based on an underlying assumption of all counterfeiting and piracy in the range of "5 to 7 percent of world trade" (Spink and Levente Fejes 2012). The high-level statistics were conducted on a data set with a very informal and qualitative foundation. This could be considered "excessive precision."

"Analysis of Counterfeit Risks and Development of a Counterfeit Product Risk Model" (Spink 2009)

"Basics of Risk Assessment – Appropriate Precision"

An expert or group of experts can provide quick insights, as well as identify potential influences that may not show up until much later using data-intensive statistical methods. A limitation of using an expert's judgment is the role assumptions play in the judgment. Techniques that simplify an analysis can compound into greater uncertainty in the final output of the model (Claycamp 2006; CODEX 2014). Usually, these heuristically-derived assumptions (e.g., using expert judgment rather than hard, unchanging data) are not clearly defined in the statistical review, and yet reports presenting the results as very precise.

In the report "Understanding Risk," the National Research Center (NRC) at the National Academies of Science discussed related analysis that is conducted to reduce the complexity of the model, and the danger that is

(continued)

oversimplifying complex, multidimensional problems can lead to results that are "highly contentious" to the decision-making process (NRC 1996).

Additional insight includes (Hassenzahl 2006):

Risk analysts are often asked to generate precise numerical calculations. The expectation serves an essential role in risk evaluations by forcing discipline on the analysts. At the same time, however, the act of generating such precise numerical calculations permits the unfortunate possibility that the resulting estimates will be interpreted as sufficient and accurate depictions of the risk. Alternatively, analysts may feel compelled to present estimates that are more precise than they feel is warranted. Stripped of quantitative and qualitative information about uncertainty, these precise estimates may become repeatedly mentioned and thereafter be interpreted as the "true" or "actual" value of the risk.

The concern is that the analysis may reach a point of "excessive precision" or a "false sense of precision and it is an important point to remember in making preliminary risk assessments or in reviewing emerging risks (Pittinger et al. 2003; Jablonowski 2005; Hassenzahl 2006).

Sidebar: Perceived Risk, Trust and Confidence, Source Credibility, and Dread and Outrage

Several key definitions and concepts from "What Role Can We Count on Consumer to Pay in Product Authentication" (MSU-FFI 2018):

Perceived Risks. The types of consumers and ways consumers respond are important base concepts, especially when dealing with perceived risk. ***Perceived risk*** is a specific consumer behavior concern which is "expected negative consequences of performing an activity such as purchasing a product"(Peter and Olsen 2005). There is a large body of research on perceived risk from a consumer behavior and a risk assessment perspective (Green et al. 1972; Gorn 1982; Haley 1995; Green et al. 2000; Haimes 2009; Lewis and Tyshenko 2009; Lindell et al. 2009; Terpstra et al. 2009; Venables et al. 2009). The intensity of the risk is influenced by the severity and the probability of the negative event (Kearny 2009; Cox 2009; Meijnders et al. 2009). "Risk depends on more than frequency and severity of consequences"(Cox 2009).

Trust and Confidence. There is research on the trust or confidence in a product or provider of products (Gotlieb and Sarel 1991; Tyler and Degoey 1996; Andrew et al. 1999; Kramer 1999; Cvetkovich et al. 2002; White et al. 2003; Chen 2008; Eitzinger and Wiedemann 2008; Sanquist et al. 2008; Earle 2009; Malka et al. 2009; Meijnders et al. 2009). Trust is usually associated with companies or agencies whereas confidence associated with an evaluation or technical assessment (Earle 2009). Trust and confidence are heavily correlated to a consumer's world view or personal experiences (Schoell and Binder 2009). In high-counterfeit markets or products, increased communication of the risks can increase consumer confidence. Consumers have a higher confidence in science confirming a risk rather than science confirming the absence of a risk (Siegrist and Cvetkovich 2001; Schoell and Binder 2009). It is easier to confirm a risk than confirm a lack of a risk (Keller et al. 2009).

Source Credibility. Source credibility, or source dynamism, is an important concept when communicating to consumers (Berlo et al. 1969; Chaiken and Maheswaran 1994; Van Kleef et al. 2007; Malka et al. 2009; Meijnders et al. 2009). Here, again, a consumer's perception could be swayed by world view or personal experiences (Burgoon et al. 1990; Gotlieb and Sarel 1991; Gotlieb et al. 1992; Stern 1994; Magee and Kalyanaraman 2007). There has been specific research on how corporations are, or are not, trusted (Kopalle and Assuncao 2000; Lafferty et al. 2002). A Harris poll identified low trust of the message of some agencies and of messages from companies (Harris Interactive 2008). In the high counterfeit markets or products, government messages about counterfeits or authentication are perceived as trusted public health promotion. "Prevention campaigns should systematically incorporate and respond to at-risk population's existing beliefs, emotions, and perceived barriers in the message design process to effectively promote behavior change"(Cho and Witte 2005).

Dread and Outrage. There is a specific study of hazard and outrage, which is also referred to as dread. Specifically, Sandman (2004a, b) developed the formula that for consumer "risk = hazard + outrage" (Sandman 1988; Sandman et al. 1993; Sandman 2004a, b; Cho and Witte 2005). The emotional concept of "dread" leads consumers to underreact to a high hazard/low outrage, such as snowboarding (Sandman 2004a, b). Consumers overreact to a low hazard/high outrage, such as terrorism (Sandman 2004a, b). Risks out of the control of the consumer, involuntary, are more of an outrage (Levitt and Dubner 2005). Generally, counterfeits in low probability markets appear to be in the low hazard/high outrage category, which would lead to a consumer overreaction.

Fear Appeals. There is a wide range of research on ***fear appeals***, also called ***fear arousal***, which use fear as a marketing tool (Tanner Jr. et al. 1991; Witte 1992; Hale and Lemieux 1995; Witte and Morrison 2000; Cho and Witte 2005; Levitt and Dubner 2005; Green and Witte 2006; Nielsen and Shapiro 2007; Lapinski and Nwulu 2008; Backer-Grøndahl et al. 2009; Furukawa et al. 2009). Examples are to either stop a dangerous behavior such as smoking or to reinforce avoiding danger such as using sunscreen. Fear appeals engage two processes: danger control and fear control (Ray

(continued)

and Wilkie 1970; Witte 1992). Different consumers could respond to the same message with either the danger or fear response. The danger is more cognition and fear is more effect. For counterfeits in markets with a low probability and severity, a quantitative thinking consumer may not perceive danger. Remember that the WHO report on counterfeit medicines reported that worldwide, ~70% of counterfeits are a placebo at worst (WHO 2007) and <0.2% of the US drug market is estimated to be counterfeit (Kearny 2009).

These wide ranges of perceived risk details demonstrate the importance of engaging the discipline of consumer behavior before implementing any new warning messages.

Qualitative vs. Quantitative Assessments and Words Versus Numbers

"Analysis of Counterfeit Risks and Development of a Counterfeit Product Risk Model," a 2009 Ph.D. Dissertation by John Spink (Spink 2009):

Risk assessments do not need to strive for quantitative output (numerical data). In fact, there is a body of literature which supports qualitative (high/medium/low) output, when there is qualitative (high/medium/low) input, including agencies such as the FDA, US Office of Management and Budget (OMB), US Department of Defense (DOD), international standards organizations, and industry associations (Broder 2000; Jablonowski 1994). For example, in a CFSAN/FDA presentation, "Tools for Prioritizing Food Safety Concerns: An FDA Perspective" (Note: author Dr. Robert Buchanan was the FDA/CFSAN Senior Science adviser and Director of Science) either qualitative and quantitative tools or models for risk ranking or assessment were validated, noting that each can have their strengths and drawbacks F(Buchanan 2007). This is supported by other authors, as well (Claycamp and Hooberman 2004; Shepherd et al. 2006; Etherton et al. 2008).

In a *Risk Management* Journal study by Jablonowski (1994), a survey of risk managers found that "words" communicated the risks better than "numbers" (Jablonowski 1994). For example, it was more descriptive and helpful to call something "rare" than to refer to a "0.05" percent chance of occurrence.

The security industry also echoes the lack of detailed history. For example, the book "Risk Analysis and the Security Survey," which is recommended reading for the American Society for Industrial Security ASIS Certified Protection Professional certification, specifically addresses security-related risks that apply directly to the anti-counterfeit strategy situation (Broder 2000):

> "Threat occurrence rates and probabilities are best developed from reports of occurrences or incident reports, whenever this historical data exist. Where information does not exist, it may be necessary to reconstruct it. This can be accomplished by conducting interviews with knowledgeable persons or by projecting data based upon educated guesses, supported by studies in like industries and locations."

The review of the literature and other reports did reveal a way to specify how to separate the categories (e.g., high/medium/low) beyond stating that the categories should be spaced far enough apart to be meaningful. The categories should not be set to parts-per-trillion if the test equipment can only measure to parts-per-million (the data would be impractical to measure). Likewise, the categories should not be set, so all the responses fall into the same rank (if all are "medium" there is no differentiation).

This focus on the presentation of the data should consider the final use of the results. Presenting the data on a broad scale or bell-shaped curve can be helpful except where the results are plotted in relation to the overall risk tolerance. When plotting versus the risk tolerance then it is possible that all food fraud vulnerabilities could cluster all above or all below that threshold.

Sidebar: Risk Assessment Numerical Methods

"Analysis of Counterfeit Risks and Development of a Counterfeit Product Risk Model" (Spink 2009):

Basics of Risk Assessment – Numerical Methods

Traditional numerical models, formulated to be solved with arithmetic operations, are the focus of engineering textbooks (Capra and Canale 1998). Unlike engineering problems (e.g., will a bridge withstand a certain load?), the counterfeit risk has human factors, and there may be no physical laws in the root cause. Due to the nature of the data, even traditional "fundamental laws" (e.g., energy cannot be created or destroyed) cannot be derived from empirical tests (e.g., observation or experiment) (Capra and Canale 1998). The Counterfeit Product Risk Model [CPRM] is not a physical system or process that is easily defined for future threats [Note: the CPRM is a general model presented in the Ph.D. Dissertation and is similar to a food fraud initial screen or pre-filter assessment].

Since engineering problem-solving concepts are familiar to many of the risk assessors assigned with counterfeit risk prediction, these concepts will be reviewed for their relevance to the model:

- **Flowcharting:** While *flowcharting* of the processes can work in a very general sense for counterfeit risk, the lack of large, historical data sets reduces the effectiveness of developing numerical models.

(continued)

- **Analytical versus numerical methods:** *Analytical methods* are considered exact, approximated by linear functions, and are of limited value since most "real" problems are more complex (Capra and Canale 1998). *Numerical methods* are based on "equations, non-linearity, and complicated geometries" and are very common in engineering problem-solving (Capra and Canale 1998). Even though the numerical solutions can be quite complex, they are still an approximation. "Although perfection is a laudable goal, it is rarely, if ever, attained" (Capra and Canale 1998). Neither applies to the Counterfeit Product Risk Model due to the underlying lack of historical data and the ever-changing nature of the risk.
- **Truncation versus round-off errors:** *Truncation error* is a different concept that measures the variation in the approximation of a number and the actual number (e.g., a measured number 4.859 but truncated to 4.9) (Capra and Canale 1998). *Round-off error* is due to method or computers simplifying the data to a finite number (e.g., Pi is 3.141592653589… but rounded off to 3.14) (Capra and Canale 1998). These concepts both assume there are a large historical data sets and some accurate measure of the system. The only historical data about counterfeiting is whether the product is known to be counterfeited and how many occurrences of the fake product were identified. Thus, neither concept applies to the Counterfeit Product Risk Model [or current food fraud risk assessments].
- **Significant figures, accuracy, and precision:** *Significant figures* refer to the number of digits that can be used to represent the data point (Capra and Canale 1998). Since the actual number for a counterfeit risk calculation cannot be known, these concepts do not apply to the Counterfeit Product Risk Model.
- **Blunders," formulation errors, and data uncertainty:** Engineering problem-solving assumes that the model and assumptions are sound, but in the real world that should not be assumed.

  - ***Blunders (in risk modeling):*** are considered to be gross errors in the data gathered or models that are not fundamentally sound relative to the data collection or measurement methods (Capra and Canale 1998).
  - ***Formulation errors, or model errors:*** are from "incomplete mathematical models" (Capra and Canale 1998). If a counterfeit risk model is based on the analysis of past data, then a mathematically representative model can be developed, but in trying to predict future risks the model developed would be fundamentally incomplete. With these fundamentally incomplete models, uncertainty (bias) would be associated with the results. When the counterfeit risk is to consider future risk, the uncertainty could magnify, detracting from the value of the prediction.
  - ***Data uncertainty*** is the error from the physical data that was used to build the model (Capra and Canale 1998). The physical data used to

> build an analytical counterfeit or product fraud assessment could be both inherently uncertain and imprecise.
>
> Quantitative methods are not always the most efficient or most appropriate prediction models. Also, classical statistical methods are based on the fundamental concepts outlined above and are not practical to apply to the Counterfeit Product Risk Model. The use of classical statistical tools such as mean, standard deviation, or variance could give an impression of excessive precision.
>
> If the Counterfeit Product Risk Model used a traditional analytical or numerical model, the associated error would lead the output to be impractical in practice. This review supports using a more general, qualitative model for counterfeit risk assessment [and also, later, for product fraud including food fraud].

Key Learning Objective 2: Introduction to Data Analytics and Big Data

This section reviews the concept of data analytics and Big Data. The terms are often used casually referring to "gathering a bunch of information." Data analytics is a specific scientific field of study that includes universities that offer master's degrees and Ph.D.s on the topic. The study of data analytics includes very specific definitions and evaluations that will be presented in this section. Data analytics is a specific discipline with unique terminology and methods. The science is not to "just gather a bunch of data" and run some spreadsheet averages. The science of data analytics is critical to understand before making any decisions regarding food fraud prevention.

The Key Learning Objectives of this section are

- (1) A review of the types of assessments or, more precisely, analytics.
- (2) Then an understanding of the ways to classify the nature of the data in the "7 Vs of Big Data."
- (3) Finally, building upon the types of analytics and nature of the data an evaluation survey is presented.

Types of Analytics

It is critical not to overstate utility of the results of an assessment such as an "impression of excessive precision" (an overview summary is provided in (Spink et al. 2019)). Descriptive analytics are very valuable but not if a customer is expecting a prediction. There are three types of analysis or analytics (Schniederjans et al. 2015):

- ***Descriptive Analytics:*** This is beyond a list of events or historical past probabilities. This is defined as: "A simple statistical technique that describes what is contained in a data set or database." "To identify possible trends in large data sets or databases" (Schniederjans et al. 2015), e.g., descriptive statistics such as averages or standard of deviation, charts, graphs, sorting methods, or lists.
- ***Predictive Analytics:*** Apply statistical modeling to not only interpolate the history from the past but consider dependent and independent variables to predict future occurrences. This is defined as: "Advanced statistical, information software, or operations research methods to identify predictive variables and build predictive models to identify trends and relationships not readily observed in a descriptive analysis" (Schniederjans et al. 2015). "To build predictive models designed to identify and predict future trends" [e.g., ANOVA and multiple regression analysis].
- ***Prescriptive Analytics:*** Build upon predictive analytics assessment of future events to decide and apply resources that mitigate consequences, e.g., linear programming and decision theory (Schniederjans et al. 2015).

These are the types of conclusions and recommendations that can be drawn from large data sets. The more data—and the more accurate, precise, and certain the data—the higher-level analytics can be conducted.

Describing the Nature of the Data

Further, to describe the data and analytics in more detail, there are the "5 Vs of Big Data"—or sometimes these range from 4 to 7 and are summarized here (McAfee and Brynjolfsson 2012; Schniederjans et al. 2015; Haan et al. 2015; Meehan 2016; Sivarajah et al. 2017):

The 5 Vs of Big Data

1. ***Volume:*** the amount of data. "Big Data" is judged in terabytes or above.
   - For example, how much information is in the data set such as the number of food fraud incidents?
2. ***Velocity:*** the speed of data collection with Big Data defined in real-time or near real-time.
   - For example, how recently is information collected and how they would include recent incidents? For example, is the entire data set reviewed and updated at least monthly, weekly, daily, hourly, etc.)?
3. ***Variety:*** a range of forms including pictures, text messages, GPS signals, sensor readings, etc.

- For example, how many different data sources are used including in how many languages?

4. ***Veracity:*** the trust in the accuracy, precision, and certainty as well as if the data set is representative of the entire event.
    - For example, how complete is the data set in covering all problems in the real world and not just "everything we could find"?
5. ***Value:*** this is a rough judgment of the actual usefulness of the data set to address the specific question or the thoroughness recommendation based on this data set.
    - For example, how much more or other information would need to be collected to make a final decision such as recalling a product, putting a product on hold to conduct authenticity tests, canceling a supply contract, or contacting a government agency to report suspicious activity?

For another perspective on "data analytics" and the "Vs of Big Data," consider the US National Institute for Standards and Testing (NIST) report on "Big Data Interoperability Framework"(NIST 2015). The NIST reference is especially important due to the formal and authoritative role of the influence on US laws and integration to international standards such as ISO.

The NIST report expands the "Vs" list and provides more detail on the veracity term:

1. ***Value*** refers to the inherent wealth, economic and social, embedded in any data set (i.e., the value of the analytics to the organization, also sometimes referred to as ***validity*** [i.e., appropriateness of the data for its intended use]).
2. ***Variability*** refers to the change in other data characteristics.
3. ***Variety*** refers to data from multiple repositories, domains, or types.
4. ***Velocity*** refers to the rate of data flow.
5. ***Veracity*** refers to the accuracy of the data.
6. ***Volatility*** refers to the tendency for data structures to change over time (i.e., the tendency for data structures to change over time).
7. ***Volume*** refers to the size of the data set.

One of the most important concepts for the food fraud prevention application is veracity, so more detail is provided here:

> "***Veracity*** refers to the completeness and accuracy of the data and relates to the vernacular 'garbage-in, garbage-out' description for data quality issues in existence for a long time. If the analytics are causal, then the quality of every data element is extremely important. If the analytics are correlations or trending over massive volume datasets, then individual bad elements could be lost in the overall counts, and the trend will still be accurate. As mentioned in Section 2.2, many people debate whether "more data is superior to better algorithms," but that is a topic better discussed elsewhere." (NIST 2015)

The "Vs of Big Data" provides a framework for explaining the nature of a data set.

Table 16.1 Evaluation of the value of data regarding data analytics: types of analytics and Vs of Big Data

Product and suspicious activity: assessment of the data and "fit for purpose"	
Research question:	
Current data set (source, information, etc.):	
Type of analytics possible (descriptive, predictive, or prescriptive):	
Details of Data—5 Vs: Concept and then judge confidence in the current data set meeting the immediate need without further processing	Confidence: 1 (low) to 5 (high)
1. Value: this is a rough judgment of the actual usefulness of the data set to address the specific question or the thoroughness recommendation based on this data set	
2. Variability: this is the change in other data characteristics	
3. Volume: the amount of data. "Big Data" is judged in terabytes or above	
4. Velocity: the speed of data collection with Big Data defined in real-time or near real-time	
5. Variety: a range of forms including pictures, text messages, GPS signals, sensor readings, etc.	
6. Veracity: the trust in the accuracy, precision, and certainty as well as if the data set is representative of the entire event	
7. Volatility: refers to the tendency for data structures to change over time	
Total =	

Assessing the Value or Utility of a Data Set

If you are going for a walk outside then, you might check the weather to examine what you might expect. First, you may look outside your window. Is it raining, snowing, windy, or calm? Should you bring an umbrella with you? How long will you be away? Will you be near a shelter? Will the consequence of getting wet be bad? Would the consequence of getting wet be catastrophic? You only can assess what you can see out your window; it would be so much wiser to look at the clouds in all directions and then check a weather report.

The application to food fraud prevention is that once the specific decision is identified, then the available data can be evaluated and assess the "fit for purpose" (Table 16.1). A data set could be judged by the type of analytics possible and then a Likert scale for the Vs of Big Data.

This table is an example of how to possibly explain and present the nature of a data set regarding the appropriate application of Big Data and data analytics.

Sidebar: Review of FMEA Application to Food Fraud

There are many risk assessment models or tools that are very successfully implemented. Some provide more value in addressing food fraud prevention than others.

Excerpt from Ph.D. (Spink 2009):

Failure Modes and Effects Analysis (FMEA)

Failure Modes and Effects Analysis (FMEA) is a quality control and risk analysis system with underlying risk assessment and management concepts that are very sound and insightful, although not necessarily suited to the all-encompassing counterfeit threat [and for food fraud prevention]. FMEA is a widely used, pro-active quality tool that focuses on design improvements and physical failures (Kmenta and Ishii 2000). The FMEA failure mode is defined here:

> ***Failure Mode and Effect Analysis (FMEA):*** the manner in which a component, sub-system, or system could potentially fail to meet the design intent. The potential failure mode could also be the cause of a potential failure mode in a higher level subsystem, or system, or the effect of a lower level effect (Kmenta and Ishii 2000).

FMEA focuses on system performance by analyzing reliability, maintainability, and safety (Onodera 1997). FMEAs are most frequently used in early product development and then again in manufacturing (Onodera 1997). The FMEA system is based on data gained from known recorded failures—in the lab and in the field— which leads to the efficient use of a probabilistic approach (probabilities based on historical data) (Kara-Zaitri et al. 1991). Other reports specifically identified FMEA in manufacturing operations, focusing on "the ways equipment can fail or be improperly operated," with an emphasis on identifying the specific single component that failed (Graver 2001). FMEA is used to analyze "risk by identifying hazards and suggesting process design modifications" (Zambrano et al. 2007). The FMEA emphasis on monitoring recurring actions within a specific system is demonstrated in the abstract of the FMEA Reference manual, published by the Society of Automotive Engineers (SAE). Its focus is on "potential failure of a product/process" and identifying actions that could reduce or eliminate the failure (Society of Automotive Engineers (SAE) 2002).

The key component of FMEA is the Risk Priority Number (RPN), which is used to assess the risk using the three criteria of occurrence, severity, and detection. Detection focuses on identifying the failure before the customer receives the product.

Detection considers the physical product's development, manufacturing, and operations. FMEA is a widely used quality and risk assessment process that is event and data intense. It focuses on specific products and systems, so it does not directly apply to the Food Fraud Prevention Strategy.

To consider the challenges of the direct application of FMEA for food fraud prevention:

- While there are known "failures" (known food fraud incidents) there are actually relatively few known "recorded failures" (100's in the world not 100's per manufacturing plant)

(continued)

- There are not enough incidents to conduct a statistically significant probabilistic risk assessment
- Food fraud incident cannot be created "in the lab."
- There can be an assessment of "the ways systems fail" based on the incident reviews
- There can be monitoring on controlling the "potential failure of a product or process."
- An adaptation of the RPN can be used in terms of assessing vulnerability assessments, but there is a key concern that a numerical assessment may "imply excessive precision" – on a scale of 1 to 5 (versus very low, low, medium, high, and very high) is a 3.5 actually significantly different from 3.7? Also, by presenting an assessment of "3.7" implies the assessment is accurate to two significant digits. Even "3" – not "3.0" since "3.0 insinuates that there is confidence in stating it is not "2.9" or "3.1″ – implies accuracy to one significant digit. If the assessment is qualitative, it is clear to state that two assessments are both "Medium" rather than "3.5 and 3.7."

Thus, the *general* FMEA principles can *generally* be applied to food fraud prevention. That said there should be great care of unintentionally presenting more accuracy, precision, or certainty than intended by the risk assessor.

Key Learning Objective 3: Extreme Events, the Highly Improbable, and Black Swans

This section reviews the study of extreme events and the highly improbable that are sometimes referred to as Black Swan events.

The Key Learning Objectives of this section are

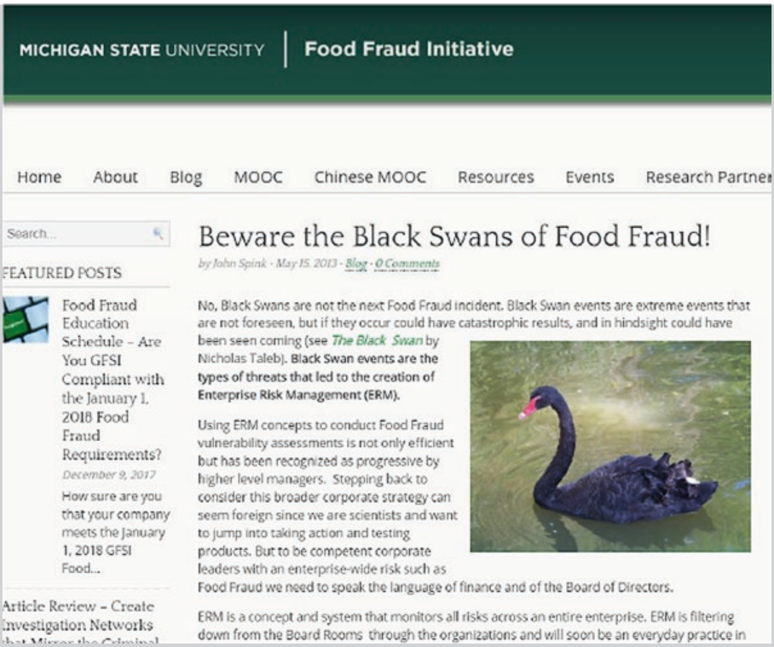
- (1) Review of extreme events and the highly improbable results
- (2) Black Swan events
- (3) The GermanWings suicidal pilot airplane crash as a Black Swan event?

Black Swan Events: The Impact of the Highly Improbable (Fig. 16.2) (MSU-FFI 2018)

Title: The Black Swans of Food Fraud

By John Spink, May 15, 2013, Blog

No, Black Swans are not the next food fraud incident. Black Swan events are extreme events that are not foreseen, but if they occur could have catastrophic results, and in hindsight could have been seen coming (see "***The Black Swan***" book by Nassim Taleb). Black Swan events are the types of threats that led to the creation of Enterprise Risk Management (ERM).



FEATURED POSTS

Food Fraud Education Schedule – Are You GFSI Compliant with the January 1, 2018 Food Fraud Requirements?

December 9, 2017

How sure are you that your company meets the January 1, 2018 GFSI Food...

Article Review – Create Investigation Networks that Mirror the Criminal

Beware the Black Swans of Food Fraud!

by John Spink · May 15, 2013 · Blog · 0 Comments

No, Black Swans are not the next Food Fraud incident. Black Swan events are extreme events that are not foreseen, but if they occur could have catastrophic results, and in hindsight could have been seen coming (see *The Black Swan* by Nicholas Taleb). **Black Swan events are the types of threats that led to the creation of Enterprise Risk Management (ERM).**

Using ERM concepts to conduct Food Fraud vulnerability assessments is not only efficient but has been recognized as progressive by higher level managers. Stepping back to consider this broader corporate strategy can seem foreign since we are scientists and want to jump into taking action and testing products. But to be competent corporate leaders with an enterprise-wide risk such as Food Fraud we need to speak the language of finance and of the Board of Directors.

ERM is a concept and system that monitors all risks across an entire enterprise. ERM is filtering down from the Board Rooms through the organizations and will soon be an everyday practice in

Fig. 16.2 Image of the blog post on the subject (Copyright Permission Granted)

Using ERM concepts to conduct Food Fraud Vulnerability Assessments are not only efficient but has been recognized as progressive by higher-level managers. Stepping back to consider this broader corporate strategy can seem foreign since we are scientists and want to jump into taking action and conducting tests of the environment. However, to be competent corporate leaders with an enterprise-wide risk such as food fraud we need to speak the language of finance and of the Board of Directors.

ERM is a concept and system that monitors all risks across an entire enterprise. ERM is filtering down from the Board Rooms through the organizations and will soon be an everyday practice in Business Units and also further down in Operations. Specifically, these enterprise-wide risks – as opposed to the more traditional operational risks – are more "vulnerabilities" than "recurring events." Their impact is more strategic than operational. An extreme event may be very unlikely but, if it occurs, could be catastrophic to the entity. For example, consider the impact on your business of the sub-prime lending crisis (economic collapse), the Japanese Tsunami and nuclear meltdown (radioactive migrating tuna), another avian influenza scare (shut down of some trade routes), or food fraud (the horsemeat scandal and the global suspicion of a food staple). The growing awareness of these types of complex risks that are distributed across an enterprise led to the creation of the ERM system and of

(continued)

a Chief Risk Officer (CRO) position. The CRO is responsible for all risks across the entire enterprise regardless of the frequency, impact, or if they have actually occurred.

It is important to emphasize that each business function is usually competently addressing risks that are clearly defined as within its roles and responsibilities. In each of the ERM examples above the food safety or Food Defense group would be competently focusing on the objective of reducing foodborne illnesses or attacks that can create public health threats – but within their boundaries what could they do about mitigating the risk of the sub-prime lending crisis?

What is unique about enterprise-wide risks is that they are often distributed across many business functions. In addition, the specific incidents are so improbable or uncontrollable that it would be inefficient for any single business function to address that vulnerability alone. That being said, the combined risk to the enterprise could be catastrophic.

What is also different about these types of strategic risks is that they are governed at the Board of Directors level (where the risk appetite and defining accountability are determined), at the Company level (where CEO and CFO evaluate the risks across the entire enterprise), and at the business unit level (where they are responsible for implementing and managing countermeasures and control systems in line with the Board of Directors and Company requirements).

Food safety professionals will find that ERM principles are similar to the International Standards Organization (ISO) standards such as ISO 31000 Risk Management and ISO 22000 Food Safety. We can also rely on best practices from ISO 27000 Information Technology Security, ISO 28000 Supply Chain Security, and the work of Technical Committee 247 on Fraud Countermeasures and Controls. All these standards also provide a framework to address the "written risk assessment" mandate in the Food Safety Modernization Act.

This is not just another version of HACCP or CARVER+Shock. Are you ready for a Black Swan event? Are you speaking the language of Enterprise Risk Management?

Sidebar: The Black Swan—"To Be Wrong with Infinite Precision"

This is a review of an idea presented by Nassim Taleb in his book *The Black Swan—The Impact of the Highly Improbable* (Taleb 2007). The analogy of a "Black Swan" is that until a swan that was black in color—rather than white—was found by explorers in Australia, the Western belief was that all swans were white. In one incident, everything changed.

One of the concepts Taleb presents is "The narrative fallacy addresses our limited ability to look at sequences of facts without weaving an explanation into them, or, equivalently, forcing a logical link, an arrow of relationship, upon them. … Where this propensity can go wrong is when it increases our impression of understanding" (Taleb 2007). This review starts with reviewing what insight is outside and inside our information set.

Insight from *outside* Our Information Set

A key point—and incredibly important challenge for food fraud prevention incident databases—is "what could be inferred from outside our information set." Often there is a lack of awareness of what is *not* included. Now, these next few thoughts seem like gibberish but follow the logic closely:

- We know what we know (also, "known-knowns).
- We don't know what we don't know (also, "unknown-knowns" or "known-unknowns").
- Wisdom comes from knowing—and to the point of assuming—we do *not* know everything.
- Further wisdom is knowing how much we do *not* know (also, "unknown-unknowns").

In that order, this seems entirely logical. That said think about some decisions made about food fraud prevention for countermeasures and control systems. There is often an unsupported assumption or stated confidence and presentation that the information set is complete. This creates Black Swan event opportunities.

Insight from *Inside* Our Information Set

A first concept is a "post hoc rationalization" where humans have a need for "sense-making" and seek logic or patterns even where there are none. An example from Taleb is first to read this statement:

A BIRD IN THE
THE HAND IS WORTH
TWO IN THE BUSH

Did you catch something wrong? In a busy world, the human brain tries to make sense of and focus on the important things. Brain scientists have found that some people have a lower rate of error in assessments based on if they are more "right brained" or "left brained." There are other interpretations and decision-making mechanisms and habits that add to the complexity. Applied to food fraud prevention, this presents interpretation bias – you might miss something obvious.

Overcausation

The world is busy, and massive amounts of information are presented. Humans need to make a lot of assumptions just to be able to walk down a hallway. Taleb stated "We [humans] harbor a crippling dislike for the abstract.

(continued)

Humans have a need to identify a root-cause to explain an event. Scientists, the public, media, and others go to great lengths to process the problem and root-cause. This is a “confirmatory bias,” “overcausation,” or “It is as if they wanted to be wrong with infinite precisions [this is sarcasm by Taleb or a statement that some risk assessors intend to deceive the reviewer].”

When there are many unknowns and uncertainty, rigorous assessments or probabilities become less and less precise and thus less valuable when selecting countermeasures and control systems. Applied to food fraud prevention, this would be trying to predict “the next melamine incident” or “which imported shipping container should we inspect.” One way to address this is to accept the uncertainty and lack of precise data. When considering what information is available there is an ability to create models that identify vulnerabilities but not necessarily probabilities. Countermeasures and control plans can be implemented that reduce *all* vulnerabilities regardless of the market dynamics or stakeholders.

The Black Swan: Experience Versus Expertise

When a new food fraud article or interview is published, there often many people who say “oh, I’ve been studying this topic for years.” Do they have “experience” or “expertise”? If they’re such experts and been working on this for so many years, then why is food fraud still a problem?

If you were leading a project to protect a bank, would you rather hire a bank manager who has “experience” being robbed or someone with “expertise” *not* being robbed? From “The Black Swan,” author Taleb would define this as two terms that which will be defined below which are the “empty-suit problem” and “epistemic arrogance” (Taleb 2007). Some key definitions help provide insight on this question (the food fraud prevention application is added for several of the key terms) (Taleb 2007):

Black Swan blindness: The underestimation of the role of the Black Swan and occasional overestimation of a specific one.

- For food fraud prevention, this would be focusing on preventing a recent incident such as melamine or horsemeat and basically ignoring trends that may identify a new “fraud opportunity.”

Black Swan ethical problem: Owing to the nonrepeatable aspect of the Black Swan, there is an asymmetry between the rewards of those who prevent and those who cure.

- For food fraud prevention, this would be the post-incident focus on detection of the specific incident rather than focusing on the root cause and general vulnerability reducing control systems.

Confirmation error (or ***platonic confirmation*** or ***confirmatory bias***): You look for instances that confirm your beliefs, your construction (or model)—and find them.

- For food fraud prevention, this could be relying heavily on a published data set to be representative of all vulnerabilities.

Empty-suit problem (or "expert problem"): Some professionals have no differential abilities from the rest of the populations but for some reason, and against their empirical records, are believe to be experts.

- For food fraud prevention, some professionals rely on their previous experience as an expert and have not reviewed new insight or methods. (It is amazing to hear absolutely positively incorrect statements made by industry experts—but the statements are made with high confidence.)

Epistemic arrogance: Measure the difference between what someone actually knows and how much they think they know. An excess will imply arrogance and a deficit of humility. An epistrocrat is someone of epistemic humility, who holds their own knowledge in greatest suspicion.

- For food fraud prevention, this could be a professional who has worked in food adulterant detection, and there is a belief that the food fraud prevention, opportunity reducing countermeasures, and control systems are from within their area of expertise (e.g., a food scientist who applies food safety microbiological prevention techniques to the human criminal adversary).

Gray Swan (Mandelbrotian): Black Swans that we can somewhat take into account—earthquakes, blockbuster books, and stock market crashes—but for which it is not possible to completely figure out the properties and produce precise calculations or probabilities.

- For food fraud prevention, the reality is that almost every single incident is a "Gray Swans" with an inevitability or warning signs. The incidents may even be "White Swans" if we assume they will eventually occur. Earthquakes do occur. Depending on the geographic location of your building, you will take more or fewer precautions.

Ludic fallacy (or uncertainty of the nerd): The manifestation of the Platonic fallacy in the study of uncertainty, basing studies of chance on the narrow world of games and dice. A-Platonic randomness has an additional layer of uncertainty concerning the rules of the game in real life. The bell curve (Gaussian), or GIF (Great Intellectual Fraud), is the application of the ludic fallacy to randomness.

- For food fraud prevention, this could be when a food safety or risk scientist applies statistical methods to a data set that is not appropriate or that is incomplete. For example, the most complex statistical analysis is usually based on the underlying assumptions of "5 to 7 percent of world trade" (Spink and Levente Fejes 2012).

Narrative fallacy: Our need to fit a story or pattern to a series of connected or disconnected facts. The statistical application is data mining.

- For food fraud prevention, this could be addressing the food fraud problem with current data sets or within current countermeasures systems. This could include food fraud being addressed in food safety early warning systems.

Reverse-engineering problem: It is easier to predict how an ice cube would melt into a puddle than, looking at a puddle, to guess the shape of the ice cube that may have caused it ("the melting ice cube"). The "inverse problem" makes narrative disciplines and accounts (such as histories) suspicious.

- For food fraud prevention, there are sometimes data sets that use themselves to validate the model (in sometimes unintentional or ignorance of circular references). For example, predicting the type of food fraud once fraud has been identified—the primary challenge is not really what type of fraud is occurring but to figure, first, if fraud is occurring. Another example is to use a known data set to create a model and then demonstrate the accuracy and precision by running examples from that data set.

Others include:

Frequency* vs. *probability: "Overconfidence is less significant when the problem is expressed in frequencies as opposed to probabilities." This also applies to vulnerabilities rather than risks or a probabilistic risk assessment.

Lack of awareness of ignorance: "In short, the same knowledge that underlies the ability to produce correct judgment is also the knowledge that underlies the ability to recognize correct judgment. To lack the former is to be deficient in the latter".

Overconfidence: "Overconfidence can be influenced by item difficulty; it typically diminishes and turns into under-confidence in easy items."

Randomness as incomplete information: Simply, what I cannot guess is random because my knowledge about the causes is incomplete, not necessarily because the process has truly predictable properties.

Retrospective distortion: Examining past events without adjusting for the forward passage of time. It leads to the illusion of posterior predictability.

Uncertainty of the deluded: People who tunnel on sources of uncertainty by producing precise sources like the great uncertainty principle, or similar, less consequential matters, to real life; worrying about subatomic particles while forgetting that we can't predict tomorrow's crises.

The Problem of Induction: "Things cannot be known with perfect certainty because their causes are infinite."

A new appreciation for our assumptions or bias is helped when stepping back and reviewing broader risk assessment concept such as the Black Swan definitions.

Sidebar: The Black Swan—"The Melting Ice Cube"

This is a review of the concept presented by Taleb in "The Black Swan" (Taleb 2007). This is one of the most effective and simple explanations to reinforce the focus on vulnerability reduction rather than specific event detection. The analogy explains a "forward process" and "backward process." He states "The backward process is much more complicated. The forward process is generally used in physics and engineering; the backward process in nonrepeatable, nonexperimental historical approaches. In a way, the limitations that prevent us from un-laying an egg also prevents us from reverse engineering history" (Taleb 2007).

Option 1 "The Melting Ice Cube": place an ice cube on a table and imagine the puddle that will result.

- For food fraud prevention we know there will—or could—be a puddle in the future. A focus could be keeping the ice cube in the freezer or to contain the puddle once it is formed. The melting ice cube and the damage from the puddle are vulnerabilities. Crime prevention theory would identify characteristics of the situation or environment that lead to the ice cube being removed and left to melt. The focus can be on reducing those root causes for a range of problems related to the access to the freezer.

Option 2 "Where did the water come from": try to reconstruct the shape of the ice cube be analyzing the puddle. This assumes the puddle is from the ice cube.

- For food fraud prevention, if there was an ice cube, there are infinite possibilities for the shape if there was, in fact, an ice cube, to begin with. Authentication would tell us that there is a puddle and that the liquid is water that is similar to what was used to make ice cubes. Control systems could tell us that an ice cube was removed from a freezer. The focus would be on alerting us when an ice cube has been attacked.

To be proactive and focus on prevention is to take the "forward process." To detect and to deter is, of course, important, but the real focus is on prevention.

A Black Swan Event?: Review of the Germanwings Airplane Crash (MSU-FFI 2018)

Title: Germanwings Airplane Crash: Was it a Black Swan Event? Was it a "Reasonably Foreseeable Hazard" or "Reasonably Likely to Occur"?

By John Spink • March 31, 2015 • Blog

(continued)

Was last week's Germanwings intentional airplane crash by a rogue pilot a "reasonably foreseeable hazard"? Was it "reasonably likely to occur"? What is the regulatory or jury-determined legal liability expectation of what is "reasonably" and "likely"? For food fraud prevention: To-be-determined.

The Germanwings plane crash from last week is a horrible tragedy on many fronts. The cause points to an intentional act by the co-pilot. The result was the crash and death of all 150 people on board. The co-pilot had a medical condition (still undefined but there is speculation) that he did not reveal to the employer. Investigators stated they found a torn-up doctor's note stating the co-pilot was "… too ill to work, including on the day of the crash."

It was reported that "Some international airlines responded to the crash by introducing new rules requiring that two crew members always be present in the cockpit. The airlines that said they were instituting a two-person rule in the cockpit included Air Canada, EasyJet, and Norwegian Air Shuttle." "The European Aviation Safety Agency [EASA], based in Cologne, Germany, also advised airlines across the region to adopt a two-person rule. The agency said the recommendation was temporary, pending the outcome of the French investigation into the Germanwings crash."

This article reviewed seemingly related suspicious airplane crashes which were:

- 2013: Mozambique Airlines, Dead: 33, "When the flight's co-pilot left to use the lavatory, the captain locked him out of the cockpit and manually steered the plan downward."
- 1999: EgyptAir, Dead: 217, "Investigators conclude that the most likely explanation was that that co-pilot, … deliberately brought down the plane… The flight data recorder showed that he waited for the captain to leave the cockpit and then disengaged the autopilot."
- 1997: Dead: 104, "[The plane] was cruising at 35,000 feet when it suddenly dove… [The pilot] had recently been demoted and disciplined by the airline and had large gambling debts."
- 1994: Air Morocco, Dead: 44, "The pilot… intentionally disconnected the plane's automatic navigation system… and crashed the plane… shortly after takeoff…"
- 1992: Japan Air Lines, Dead: 24 of 166 passengers, "…the pilot… sent the plane into Tokyo Bay moments before it was to land… He had a history of 'psychosomatic disorders' in the late 1980s, but airline doctors said he was fit for duty."

So, after considering this new information, is the suicidal pilot risk a Reasonably Foreseeable Hazard or Reasonably Likely to Occur?

This incident raises some interesting questions about the definition of what is a "reasonably foreseeable hazard" and what is "reasonably likely to occur." This incident also provides an example of the difference between: (1) the need or expectation to address a hazard and (2) knowledge that an incident could occur. The data is that there were five (5) related suspicious airplane crashes in the last 23 years. Though it could be argued that a Probabilistic Risk Assessment would be an inappropriate assessment for this type of "vulnerability" there would have been an infinitesimal probability of this incident occurring. That said, the intentional airplane crashes are not unheard of.

FDA Food Protection Plan: Intervention, Response, and to Prevention

For food fraud prevention we have discussed the process of prevention to intervention to response. We note that after a new incident the process starts at Intervention, then to Response, and finally back up to Prevention. By definition, the new incident either defines a previously unheard-of risk (e.g., a "Black Swan" event) or provides new information on a previously known risk (e.g., a "Gray Swan" event). (Note: see the previous blog post on "Beware the Black Swans of Food Fraud.")

Intervention

- This Incident: The plane has already crashed. The incident has passed. There is no "Intervention" for this incident.
- Future Incidents: This would focus on how to intervene in future situations where a pilot may try to take over the cockpit. Actually, expand this to anyone with access to the cockpit including other staff or a passenger. There are times during a flight when the cockpit door does open. The health of the pilot would also be a consideration, but that is more "traditional criminology" focusing on the perpetrator, not "environmental criminology" focusing on managing the "space" of the crime – Situational Crime Prevention. The company has more control over the physical space of the crime rather than of the perpetrators.

Response

- This Incident: This incident has passed so no "Response."
- Future Incidents – Immediate: Airlines and the EASA have implemented a temporary mandatory requirement that two pilots be in the cockpit at all times even if this means a third pilot is required on a flight. (This will be interesting on flights where there are only two seats in the cockpit.)
- Future Incidents – Future: This would technically be addressed under the Prevention category.
- In General: It appears that the Response for this and other incidents is related to the catastrophic nature of the risk and the clarity of the immediate effect of a countermeasure. Requiring two pilots to be in an airplane cockpit can be implemented immediately, and there is logic to how this reduces the "crime opportunity."

(continued)

Prevention

- Future Incidents: It appears longer-term research into Prevention is already underway. The “two-pilot” rule may become – or may just have become – a standard industry practice.

The Germanwings airplane crash provides a case study to define the nuance of “reasonably foreseeable hazard” and “reasonably likely to occur.” For food fraud prevention this incident emphasizes the importance of taking the time and effort to thoroughly and precisely define the fundamental concepts. While this will require a lot more consideration and research, this incident seems to emphasize a focus on prevention and reducing vulnerabilities. For food fraud prevention these are already core, fundamental concepts. MSU-FFI

Conclusion

This second risk analysis chapter expanded on the basic fundamentals to an application to food fraud prevention. Through a series of basic concepts, and application examples, consistent and revealing practical and pragmatic insights can be found. ***The first conclusion is*** that food fraud is a new and different type of food risk so the “it” in “do it right the first time” is to *only* conduct a PRELIMINARY review…at least for now. There is an expectation that the insights will probably reveal very different types of best practices. This leads to an insight that at different stages in the implementation there are very different needs from the data (e.g., accuracy, precision, certainty, and robustness). Also, due to the nature of the data sets and the assessments, seemingly simplistic qualitative assessments and presentations may be optimal. ***The second conclusion is*** that all data analysis should include basic data analytics/Big Data review. Often, due to the nature of food fraud and the fraud act compared to other problems, there is a massively smaller data set with exponentially less thorough information. It is critical to characterize the nature of the data to explain the level of output that can be expected. Often for food fraud, there is so little data that there is almost never enough for a “prescriptive analytics” or “predictive analytics” and often not even enough to state a statistical significance meaningful “descriptive analytics.” There is absolutely enough information and data to conduct incident reviews that explain the system weaknesses such as in the Product Counterfeiting Incident Clustering Tool (PCICT) or Hot Product and Hot Spot analysis. ***The final conclusion is*** that there are great insights to be gained from the study of extreme events and the research on the highly improbable. Many food fraud incidents fall into the realm of Black Swan events. Once there is a realization of being in “Extremistan,” there is a new perspective, theories, and models to apply. With the right perspective and vulnerability assessment, there is shift from being surprised by Black Swan events to seeking Gray Swans—a shift from mitigation (a quick response to minimize the negative consequences of an event after it has occurred) to prevention (reducing system weaknesses to try to prevent the event from even being able to occur). There is a saying:

> ***Avoid presenting the "impression of excessive precision" and the temptation "to be wrong with infinite precision."***

Appendix: WIIFM Chapter on Risk Application

This "What's In It For Me" (WIFFM) section explains why this chapter is important to you.

Business functional group	Application of this chapter
WIIFM all	There are very different work processes, but they are key to addressing these highly improbable but often catastrophic Black Swan-type events
Quality team	There are very specific risk analysis and risk assessment methods that apply and do *not* get overly complex until you conduct high-level, prefilter information gathering projects
Auditors	Due to the nature of the risk—and the current GFSI requirements—the assessments will seem extremely simple and light compared to other HACCP-type assessments
Management	Support the continuous review of the process with a series of lighter activities and deliverables—"do it right the first time" is to conduct enterprise-wide assessment that is not very certain or robust, yet
Corp. decision-makers	The first assessments will be light but effective, for now

Appendix: Study Questions

This section includes study questions based on the key learning objectives in this chapter:

1. Discussion Question
   (a) When considering data needs, what is the relationship between accuracy, precision, and certainty?
   (b) When presenting FF vulnerabilities, what are the strengths and weaknesses of "qualitative versus quantitate" and "words versus number"?
   (c) How do the concepts of Black Swans, Gray Swans, and White Swans apply to FF prevention?

2. Key Learning Objective 1
   (a) What is “data uncertainty”?
   (b) How does “dread and outrage” impact the reponses to a FF incident?
   (c) How do “blunders” impact the effectiveness of addressing FF prevention?
3. Key Learning Objective 2
   (a) What is “data veracity”?
   (b) What are the “7 Vs of data analytics”?
   (c) Are most FF vulnerability assessments “descriptive,” “predictive,” or “prescriptive” analytics or none of the above?
4. Key Learning Objective 3
   (a) How did the “Black Swan event” get its name?
   (b) What is “experience vs. expertise”?
   (c) What does mean to be “wrong with infinite precision”?

References

Andrew, P. S., Young, J. A., & Gibson, J. (1999). How now, mad-cow? Consumer confidence and source credibility during the 1996 BSE scare. *European Journal of Marketing, 33*(11/12), 1107.

Backer-Grøndahl, A., Fyhri, A., Ulleberg, P., & Amundsen, A. (2009). Accidents and unpleasant incidents: Worry in transport and prediction of travel behavior. *Risk Analysis, 29*(9), 1217.

Berlo, D. K., Lemert, J. B., & Mertz, R. J. (1969). Dimensions for evaluating the acceptability of message sources. *Public Opinion Quarterly, 33*(4), 563–576.

Broder, J. F. (2000). *Risk analysis and the security survey*. Boston: Butterworth-Heineman.

Buchanan, R. (2007). *Tools for prioritizing food safety concerns: An FDA perspective. Tools for prioritizing food safety concerns workshop*. Greenbelt: CFSAN/FDA, JIFSAN.

Burgoon, J. K., Birk, T., & Pfau, M. (1990). Nonverbal behaviors, persuasion, and credibility. *Human Communication Research, 17*(1), 140.

Capra, S., & Canale, R. (1998). *Numerical methods for engineers*. Boston: McGraw-Hill.

Chaiken, S., & Maheswaran, D. (1994). Heuristic processing can bias systematic processing: Effects of source credibility, argument ambiguity, and task importance on attitude judgment. *Journal of Personality and Social Psychology, 66*, 460–473.

Chen, M. (2008). Consumer trust in food safety–A Multidisciplinary Approach and Empirical evidence from Taiwan. *Risk Analysis, 28*(6), 1553.

Cho, H., & Witte, K. (2005). Managing fear in public health campaigns: A theory-based formative evaluation process. *Health Promotion Practice, 6*(4), 482.

Claycamp, H. G. (2006). Rapid benefit-risk assessments: No escape from expert judgments in risk management. *Risk Analysis, 26*(1), 147–156.

Claycamp, H. G., & Hooberman, B. H. (2004). Antimicrobial resistance risk assessment in food safety. *Journal of Food Protection, 67*, 2063–2071.

CODEX, Codex Alimentarius. (2014). *Procedural manual, twenty-second edition*. Geneva/Rome: World Health Organization/Food and Agriculture Organization of the United Nations.

Cox, A. L. (2009). Some limitations of frequency as a component of risk: An expository note. *Risk Analysis, 29*(2), 171.

Cvetkovich, G., Siegrist, M., Murray, R., & Tragesser, S. (2002). New information and social trust: Asymmetry and perseverance of attributions about hazard managers. *Risk Analysis, 22*(2), 359–367.

Earle, T. (2009). Trust, confidence, and the 2008 global financial crisis. *Risk Analysis, 29*(6), 785.

Eitzinger, C., & Wiedemann, P. (2008). Trust in the safety of tourist destinations: Hard to gain, easy to lose? New insights on the asymmetry principle. *Risk Analysis, 28*(4), 843.

Etherton, J., Main, B., Cloutier, D., & Christensen, W. (2008). Reducing risk on machinery: A field evaluation pilot study of risk assessment. *Risk Analysis, 28*(3), 711–721.

Furukawa, K., Cologne, J., Shimizu, Y., & Ross, N. (2009). Predicting future excess events in risk assessment. *Risk Analysis, 29*(6), 885.

Gorn, G. J. (1982). The effects of music in advertising on choice behavior: A classical conditioning approach. *Journal of Marketing, 46*(1), 94.

Gotlieb, J. B., & Sarel, D. (1991). Comparative advertising effectiveness: The role of involvement and source credibility. *Journal of Advertising, 20*(1), 38.

Gotlieb, J. B., Schlacter, J. L., & St Louis, R. D. (1992). Consumer decision making: A model of the effects of involvement, source credibility, and location on the size of the price difference required to induce consumers to change suppliers. *Psychol Mark (1986–1998), 9*(3), 191.

Graver, P. A. (2001). *Process hazard analysis – Failure Mode Effects Analysis (FMEA)*. FMEA Information Center. https://www.scribd.com/document/62815282/FMEA-Example-1

Green, E. C., & Witte, K. (2006). Can fear arousal in public health campaigns contribute to the decline of HIV prevalence? *Journal of Health Communication, 11*(3), 245–259.

Green, P. E., Wind, Y., & Jain, A. K. (1972). Benefit bundle analysis. *Journal of Advertising Research, 12*(2), 31.

Green, P. E., Wind, Y., & Jain, A. K. (2000). Benefit bundle analysis. *Journal of Advertising Research, 40*(6), 32–37.

Haan, J., Rodammer, F., & Speier-Pero, C. (2015). The integration of business analytics into a business college undergraduate curriculum.

Haimes, Y. (2009). On the definition of resilience in systems. *Risk Analysis, 29*(4), 498.

Hale, J. L., & Lemieux, R. (1995). Cognitive processing of fear-arousing message content. *Communication Research, 22*(4), 459.

Haley, R. I. (1995). Benefit segmentation: A decision-oriented research tool. *Marketing Management, 4*(1), 59–62.

Hassenzahl, D. M. (2006). Implications of excessive precision for risk comparisons: Lessons from the past four decades. *Risk Analysis, 26*(1), 265–276.

Harris Interactive. (2008). *Confidence in FDA hits new low, according to WSJ.com/Harris interactive study (Harris Poll): U.S. adults concerned about safety of prescription drugs*. Rochester: Harris Interactive.

Jablonowski, M. (1994). Words or numbers? *Risk Management, 41*(12), 47.

Jablonowski, M. (2005). Do catastrophe models mislead? *Risk Management, 52*(7), 32.

Kara-Zaitri, C., Keller, A. Z., Barody, I., & Fleming, P. V. (1991). An improved FMEA methodology. Reliability and Maintainability Symposium. *Proceedings Annual 1991*, Orlando, FL, 248–252.

Kearny, A. T. (2009). *Presentation, quoting pharmaceutical security institute (PSI)*. Washington, DC: GMA Economically Motivated Aduleration Working Group.

Keller, C., Siegrist, M., & Visschers, V. (2009). Effect of risk ladder format on risk perception in high- and low-numerate individuals. *Risk Analysis, 29*(9), 1255.

Kmenta, S., & Ishii, K. (2000). Scenario-based FMEA: A life cycle cost perspective 2000. In *ASME Design Engineering Technical Conferences*. Baltimore, Maryland, ASME.

Kopalle, P. K., & Assuncao, J. L. (2000). When (not) to indulge in “puffery”: The role of consumer expectations and brand goodwill in determining advertised and actual product quality. *Managerial and Decision Economics, 21*(6), 223.

Kramer, R. M. (1999). Trust and distrust in organizations: Emerging perspectives, enduring questions. *Annual Review of Psychology, 50*(1), 569–598.

Lafferty, B. A., Goldsmith, R. E., & Newell, S. J. (2002). The dual credibility model: The influence of corporate and endorser credibility on attitudes and purchase intentions. *Journal of Marketing Theory and Practice, 10*(3), 1.

Lapinski, Maria Knight and P. Nwulu (2008). Can a short film impact HIV-related risk and stigma perceptions? Results from an experiment in Abuja, Nigeria. Health Communication. 23(5): 403–412.

Levitt, S. D., & Dubner, S. J. (2005). *Freakonomics*. New York: HarperCollins.

Lewis, R., & Tyshenko, M. (2009). The impact of social amplification and attenuation of risk and the public reaction to mad cow disease in Canada. *Risk Analysis, 29*(5), 714.

Lindell, M., Arlikatti, S., & Prater, C. (2009). Why people do what they do to protect against earthquake risk: Perceptions of hazard adjustment attributes. *Risk Analysis, 29*(8), 1072.

Magee, R., & Kalyanaraman, S. (2007). Antecedent variables in persuasion processes: The effect of worldview on the processing of persuasive messages. Conference Papers – International Communication Association, International Communication Association.

Malka, A., Krosnick, J., & Langer, G. (2009). The association of knowledge with concern about global warming: Trusted information sources shape public thinking. *Risk Analysis, 29*(5), 633.

McAfee, A., & Brynjolfsson, E. (2012). Big data: The management revolution. (cover story). *Harvard Business Review, 90*(10), 60–68.

Meehan, T. (2016). What is Big Data? Loss prevention. January–February: 1.

Meijnders, A., Midden, C., Olofsson, A., Öhman, S., Matthes, J., Bondarenko, O., Gutteling, J., & Rusanen, M. (2009). The role of similarity cues in the development of trustin sources of information about GM food. *Risk Analysis, 29*(8), 1116.

MSU-FFI, Food Fraud Initiaive (2018). Blog series, Food Fraud Initiative, Michigan State University, developed and presented by John Spink, URL: www.FoodFraud.msu.edu/Blog/.

Nielsen, J., & Shapiro, S. (2007). Side effects from fear: The automatic inhibition of threat-relevant brand advertising. *Advances in Consumer Research, 34*, 192.

NIST, United States National Institute of Science and Technology (2015). NIST Big Data interoperability framework Big Data Public Working Group, Special publication, URL: https://bigdatawg.nist.gov/_uploadfiles/NIST.SP.1500-1.pdf. Special Publication: 1500–1506.

NRC, National Research Council. (1996). In P. C. Stern & H. V. Fineberg (Eds.), *Understanding risk: Informing decisions in a democratic society, National Academy of Science NAS*. Washington, DC: National Academies Press.

Onodera, K. (1997). Effective techniques of FMEA at each life-cycle stage. Reliability and Maintainability Symposium. *1997 Proceedings Annual,* pp. 50–56.

Peter, J. P., & Olsen, J. C. (2005). *Consumer behavior & marketing strategy*. New York: McGraw-Hill Irwin.

Pittinger, C. A., Brennan, T. H., Badger, D. A., Hakkinen, P. J., & Catherine Fehrenbacher, M. (2003). Aligning chemical assessment tools across the hazard-risk continuum. *Risk Analysis, 23*(3), 529–535.

Ray, M. L., & Wilkie, W. L. (1970). Fear: The potential of an appeal neglected by marketing. *American Marketing Association., 34*, 54–62.

Sandman, P. M. (1988). Risk communication: Facing public outrage. *Management Communication Quarterly, 2*(2), 235.

Sandman, P. M. (2004a). July 2004 issue of the synergist, pp. 24–25, http://www.psandman.com/col/under-r.htm.

Sandman, P. M. (2004b). The synergist, February 2004 issue of the synergist, pp. 22, 24. http://www.psandman.com/col/over-re.htm.

Sandman, P. M., Miller, P. M., Johnson, B. B., & Weinstein, N. D. (1993). Agency communication, community outrage, and perception of risk: Three simulation experiments. *Risk Analysis, 13*(6), 585–598.

Sanquist, T., Mahy, H., & Morris, F. (2008). An exploratory risk perception study of attitudes toward homeland security systems. *Risk Analysis, 28*(4), 1125.

Schniederjans, M. J., Schniederjans, D. G., & Starkey, C. M. (2015). *Business analytics principles, concepts, and applications: What, why, and how*. Upper Saddle River: Pearson Education.

Schoell, R., & Binder, C. (2009). System perspectives of experts and farmers regarding the role of livelihood assets in risk perception: Results from the structured mental model approach. *Risk Analysis, 29*(2), 205.

Shepherd, R., Barker, G., French, S., Hart, A., Maule, J., & Cassidy, A. (2006). Managing food chain risks: Integrating technical and stakeholder perspectives on uncertainty. *Journal of Agricultural Economics, 57*(2), 313–327. https://doi.org/10.1111/j.1477-9552.2006.00054.

Siegrist, M., & Cvetkovich, G. (2001). Better negative than positive? Evidence of a bias for negative information about possible health dangers. *Risk Analysis, 21*(1), 199–206.

Sivarajah, U., Kamal, M. M., Irani, Z., & Weerakkody, V. (2017). Critical analysis of big data challenges and analytical methods. *Journal of Business Research, 70*, 263–286.

Society of Automotive Engineers (SAE) (2002). Potential failure mode and effects analysis in design (Design FMEA) and potential failure mode and effects analysis in manufacturing and assembly processes (Process FMEA). Reference manual, Document number: SAE J 1739.

Spink, J. (2009). *Analysis of counterfeit risks and development of a counterfeit product risk model*. PhD dissertation Ph.D., Michigan State University.

Spink, J. (2014). Food Fraud prevention overview, introducing the Food Fraud Prevention Cycle (FFPC)/Food Fraud Prevention System, GFSI China focus day 2014, Beijing.

Spink, J., & Levente Fejes, Z. (2012). A review of the economic impact of counterfeiting and piracy methodologies and assessment of currently utilized estimates. *International Journal of Comparative and Applied Criminal Justice, 36*(4), 249–271.

Spink, J., Elliott, C., Dean, M., Speier-Pero, C. (2019). Fraud Data Collection Needs Survey, *NPJ Science of Food, 3*(1), Pages 1–8 [Available on-line May 16, 2019].

Spink, J., Zhang, G., Chen, W., & Speier-Pero, C. (2019). Introducing the food fraud prevention cycle (FFPC): A dynamic information management and strategic roadmap. *Food Control, 105*, 233–241.

Stern, B. B. (1994). A revised communication model for advertising: Multiple dimensions of the source, the message, and the recipient. *Journal of Advertising, 23*(2), 5.

Taleb, N. N. (2007). *The black swan: The impact of the highly improbable*. New York: Random house.

Tanner, J. F., Jr., Hunt, J. B., & Eppright, D. R. (1991). The protection motivation model: A normative model of fear appeals. *Journal of Marketing, 55*(3), 36.

Terpstra, T., Lindell, M., & Gutteling, J. (2009). Does communicating (flood) risk affect (flood) risk perceptions? Results of a quasi-experimental study. *Risk Analysis, 29*(8), 1141.

Tyler, T. R., & Degoey, P. (1996). Trust in organizational authorities. In *Trust in organizations: Frontiers of theory and research* (pp. 331–356). Thousand Oaks: Sage Publications.

Van Kleef, E., Houghton, J. R., Krystallis, A., Pfenning, U., Rowe, G., Van Dijk, H., Van der Lans, I. A., & Frewer, L. J. (2007). Consumer evaluations of food risk management quality in Europe. *Risk Analysis, 27*(6), 1565–1580.

Venables, D., Pidgeon, N., Simmons, P., Henwood, K., & Parkhill, K. (2009). Living with nuclear power: A Q-method study of local community perceptions. *Risk Analysis, 29*(8), 1089.

White, M. P., Pahl, S., Buehner, M., & Haye, A. (2003). Trust in risky messages: The role of prior attitudes. *Risk Analysis, 23*(4), 717–726.

WHO, World Health Organization (2007). General information on counterfeit medicines World Health Organization. 2007.

Witte, K. (1992). Putting the fear back into fear appeals: The extended parallel process model. *Communication Monographs, 59*(4), 329.

Witte, K., & Morrison, K. (2000). Examining the influence of trait anxiety/repression-sensitization on individuals' reactions to fear appeals. *Western Journal of Communication, 64*(1), 1.

Zambrano, L., Sublette, K., Duncan, K., & Thoma, G. (2007). Probabilistic reliability modeling for oil exploration & production (E&P) facilities in the tallgrass prairie preserve. *Risk Analysis, 27*, 1323–1333.