Cybersecurity and the Role of the Food Safety Manager
(Post Workshop Update)

Food Fraud Prevention ACADEMY

John W Spink, Ph.D.
Director, Food Fraud Prevention Academy
John.Spink@YorkPartnersLLC.com
517-381-4491

Also: Assistant Professor, Department of
Supply Chain Management, Business College,
Michigan State University (USA)

Food Safety Summit 2022
Rosemont, Illinois
Tues, May 10, 2022
12:30 to 2:30pm CT (Updated)

QR   URL: Link

FoodFraudPrevention.com   Twitter: @FoodFraud   #FoodFraud

1

Food Fraud Prevention ACADEMY

From Food Fraud Prevention to Cybersecurity

- **E-Commerce and food fraud:**
  - Online marketplaces and sales channels have been a source of food fraud for counterfeit, stolen goods, diverted goods, and expired products.
  - FFVA for online sales for FSAI, Interpol/ Europol, and others.
  - Research and presentations on the impact of e-commerce on food safety and food fraud
- **ISO 22000 Food Safety Management**
  - In 2018, section 4.1 expanded to "external issues" including "cybersecurity and food fraud."
  - Question: cybersecurity and food fraud... separately or together?
- **Supply Chain Management education**
- **Vulnerability assessments** of novel events: applying FFIS, FFVA, and VACCP

Online Food Fraud

SCM Education

ISO 22000

FFVA

2   © 2022 Food Fraud Prevention Think Tank LLC   FoodFraudPrevention.com
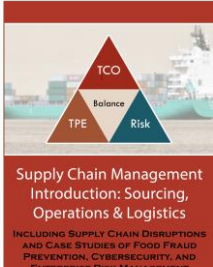
2

Food Fraud Prevention ACADEMY

New Book Chapter-Section: Cybersecurity in ISO 22000 Food Safety Management

- The foundation of this presentation is my chapter-section draft.
- Please review and comment on the chapter-section in the shared Google Document:
- https://docs.google.com/document/d/1S F9hLtO4yfvaRzPLradS9ILwnkC5E2SU/ed it?usp=sharing&ouid=106328742619920 569986&rtpof=true&sd=true

CONTRIBUTE!!!

Supply Chain Management
Introduction: Sourcing, Operations & Logistics

INCLUDING SUPPLY CHAIN DISRUPTIONS AND CASE STUDIES OF FOOD FRAUD PREVENTION, CYBERSECURITY, AND

CHAPTER 13: CYBERSECURITY

13.04   Cybersecurity in ISO 22000 Food Safety Management

3   © 2022 Food Fraud Prevention Think Tank LLC   FoodFraudPrevention.com

3

The Role of the Food Safety Manager in Cybersecurity (or vice versa)

4   © 2022 Food Fraud Prevention Think Tank LLC   FoodFraudPrevention.com

4

Food Fraud Prevention ACADEMY

Agenda

- Start with the FSMA and Food Safety Management Systems
  - ISO 22000 Food Safety Management (the foundation for GFSI and the food safety standards)
  - FSMA
- General Cybersecurity standards:
  - NIST Cybersecurity Framework
  - ISO 27000 Information Security
  - ISO 27034 Cybersecurity
  - NIST Prioritizing Cybersecurity Risk for Enterprise Risk Management (ERM)
- ***The role of the food safety manager is cybersecurity...***

5   © 2022 Food Fraud Prevention Think Tank LLC   FoodFraudPrevention.com

5

What do you need to do?

Food Safety Compliance for
- GFSI/ Food Safety Management System
- Food laws and regulations
- Corporate requirements
- Others

6   © 2022 Food Fraud Prevention Think Tank LLC   FoodFraudPrevention.com

6

Food Fraud Prevention ACADEMY

FSMA

- **FSMA-Preventive Controls – September 2016**
  - *"The hazard analysis must be written regardless of its outcome"* [21CFR507.33 (a)(2)]/ 21CFR117.130

21 USC Ch. 27: FOOD SAFETY MODERNIZATION
From Title 21—FOOD AND DRUGS

CHAPTER 27—FOOD SAFETY MODERNIZATION
SUBCHAPTER I—IMPROVING CAPACITY TO PREVENT FOOD SAFETY PROBLEMS
Sec.
2201.   Performance standards.
2202.   National Agriculture and Food Defense Strategy.
2203.   Food and Agriculture Coordinating Councils.
2204.   Building domestic capacity.
2205.   Food allergy and anaphylaxis management.
2206.   Alcohol-related facilities.

Cybersecurity Explicit or Implicit?

If it's a hazard it must be assessed.

7   © 2022 Food Fraud Prevention Think Tank LLC   FoodFraudPrevention.com

7

Food Fraud Prevention ACADEMY

GFSI Food Safety Management System

- Keywords:
  - Cyber = 0
  - Internet = 0
  - Information Technology/ IT = 0
  - *Conclusion: No cybersecurity requirements?*
- Food defence: The process to ensure the security of food, food ingredients, feed or food packaging from all forms of intentional malicious attack….
- Food safety: Assurance that any product within the GFSI scopes of recognition will not cause an adverse health effect…
- HACCP: A system which identifies, evaluates, controls and monitors hazards relating to food safety….

GFSI BENCHMARKING REQUIREMENTS
VERSION 2020

GFSI BENCHMARKING REQUIREMENTS
VERSION 2020

PART I
THE GFSI BENCHMARKING PROCESS

Explicit or Implicit?

8   © 2022 Food Fraud Prevention Think Tank LLC   FoodFraudPrevention.com

8

Food Fraud Prevention ACADEMY

Corporate or Customer Requirements

- Beyond food safety to supplier qualification.
- Information Technology/ Cybersecurity standards

BUT…
…what is the problem?
…what are the requirements for your company?
…what are the requirements for your FSMS?

9 © 2022 Food Fraud Prevention Think Tank LLC   FoodFraudPrevention.com

9

Cybersecurity Hot Topics

10 © 2022 Food Fraud Prevention Think Tank LLC   FoodFraudPrevention.com

10

Food Fraud Prevention ACADEMY

High Profile Incidents

- Solar Winds (malware, software access)
- Colonial Pipeline (ransomware, proactively shut down the entire system)
- JBS US Holdings (Ransomware, encrypted server)
- Genome Information Cybertheft
- Oldsmar Water Authority (remote access, changed levels of lye, 2017)
- AmeriCold Logistics (Ransomware, cold storage, encrypted servers)

Is the target a company/industry… or their money?

Hot topic and pressure
- FDA New Era in Smarter Food Safety, Public Meeting on E-Commerce in October 19-21, 2021.
- Note: focused on B2C commerce and food safety hazards during the preparation and delivery by new businesses
  - "e.g., produce and meal kit subscription services, ghost kitchens, dark stores),"
  - "U.S. Postal Service, UPS, FedEx, Uber, Lyft, DoorDash, etc."

Wait… Cybersecurity or e-commerce (or both)?

11 © 2022 Food Fraud Prevention Think Tank LLC   FoodFraudPrevention.com

11

Food Fraud Prevention ACADEMY

FDA New Era for Smarter Food Safety E-Commerce Meeting (E-order and delivery)

The FDA is taking a proactive first step aligned with standards such as ISO 31000 Risk Management of "establishing the context."

Following ISO 9000 Quality Management and ISO 22000 Food Safety Management, the next step is to gather incident information to conduct risk identification before considering the risk assessment models or methods.

Reference:
- https://www.blog.foodfraudpreventionthinktank.com/
- https://www.ams.usda.gov/services/organic-certification/training
- https://www.fda.gov/food/workshops-meetings-webinars-food-and-dietary-supplements/new-era-smarter-food-safety-summit-e-commerce-ensuring-safety-foods-ordered-online-and-delivered

Yes e-commerce but really a review of a novel supply chain channel. Not cybersecurity.

12 © 2022 Food Fraud Prevention Think Tank LLC   FoodFraudPrevention.com

12

ISO 22000 Food Safety Management

Voting Member, ISO TC23/WG17 (ISO 22000)

13 © 2022 Food Fraud Prevention Think Tank LLC FoodFraudPrevention.com

13

Food Fraud Prevention ACADEMY

ISO 22000 Food Safety Management

- ***Builds on ISO 9000 Quality Management, ISO 31000 Risk Management, and others.***
- International Standards Organization, Technical Committee 34 Food products, Sub-Committee 34 Management systems for food safety (ISO/TC 34/SC 17)
- Health hazards from food safety incidents
- Reduce health hazards and increase the methodology to reduce the possibility of incidents
- Focuses on health hazards, new food fraud requirements in 2018.
- ***The foundation for GSFI food safety management systems.***

"The ISO 22000 family contains a number of standards each focusing on different aspects of food safety management.
- ISO 22000:2005 contains the <u>overall guidelines</u> for food safety management.
- ISO 22004:2014 provides <u>generic advice</u> on the application of ISO 22000
- ISO 22005:2007 focuses on <u>traceability</u> in the feed and food chain
- ISO/TS 22002–1:2009 contains specific <u>prerequisites</u> for food manufacturing
- ISO/TS 22002–2:2013 contains specific prerequisites <u>for catering</u>
- ISO/TS 22002–3:2011 contains specific prerequisites <u>for farming</u>
- ISO/TS 22002–4:2013 contains specific prerequisites <u>for food packaging manufacturing</u>
- ISO/TS 22003:2013 provide guidelines for <u>audit and certification bodies."</u>

14 © 2022 Food Fraud Prevention Think Tank LLC FoodFraudPrevention.com

14

Food Fraud Prevention ACADEMY

ISO 22000: Overview

- "Introduction - 0.3.3.3 Hazard analysis — Operational processes: The concept of risk-based thinking based on the HACCP principles at the operational level is implicit in this document. The subsequent steps in HACCP can be considered as the necessary measures to prevent hazards or reduce hazards to acceptable levels to ensure food is safe at the time of consumption."

15   © 2022 Food Fraud Prevention Think Tank LLC   FoodFraudPrevention.com

15

Food Fraud Prevention ACADEMY

What is the cybersecurity requirement for ISO 22000 compliance?

The scope includes anything that could lead to a food safety-based adverse health effect.

- "4.1. The organization shall determine external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended results of its food safety management system. The organization shall identify, review and update information related to these external and internal issues."

Then Section 4.1, Note 1 clearly defines food fraud within the scope of the standard. *The standard only mentions the term once and only in a "note."*

- "Understanding the context can be facilitated by considering external and internal issues including but not limited to legal, technological, competitive, market, cultural, social, economic environments, **cybersecurity** and ***food fraud***, food defence and intentional contamination, knowledge, and performance of the organization, whether international, national, regional or local."

Together? Typo? …the "and"

16   © 2022 Food Fraud Prevention Think Tank LLC   FoodFraudPrevention.com

16

Food Fraud Prevention ACADEMY

How formal or direct are the ISO 22000 related cybersecurity requirements?

- *There are no further details or explicit compliance requirements.*
- *Iso 22000 does not have a definition of cybersecurity.*
- *Iso 28000 Supply Chain Security does not even mention cybersecurity (only IT/ ICT security)*
- *The GFSI Benchmarking document does **not** mention cybersecurity.*
- *...now what? Ignore it?*
- *...insight from where cybersecurity mentioned in ISO?*

17   © 2022 Food Fraud Prevention Think Tank LLC   FoodFraudPrevention.com

17

NIST
ISO 27000 & IS0 27001
ISO 27032 Cybersecurity

18   © 2022 Food Fraud Prevention Think Tank LLC   FoodFraudPrevention.com

18

Food Fraud Prevention ACADEMY

NIST in One Slide:
The Foundation

- US National Institute of Standards and Technology (NIST)
- US Department of Commerce, coordinates measurement standards including information security standards for federal computer systems.
- NIST Cybersecurity Framework
- Information Security Handbook: Guide for Managers (SP-800-100)
- Managing Information Security (SP-800-39)
- *...and more on the way*

19   © 2022 Food Fraud Prevention Think Tank LLC   FoodFraudPrevention.com

19

Food Fraud Prevention ACADEMY

ISO 27000 Information Security Management
ISO 27001 IS Management Systems Requirements

ISO 27000 – the series
- Management System Standard (MSS) comprised of standards including ISO 27001 requirements and ISO 27032 Information technology – Security Techniques – Guidelines for Cybersecurity (Cybersecurity).
  - ***Information Security Incident Management***: processes for detecting, reporting, assessing, responding to, dealing with, and learning from information security incidents. (REF 27000)

ISO 27001 – the requirements
- The requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization.

ISO/IEC 27001
INFORMATION SECURITY MANAGEMENT

ISO/IEC 27001:2013
Information technology — Security techniques — Information security management systems — Requirements

20   © 2022 Food Fraud Prevention Think Tank LLC   FoodFraudPrevention.com

20

Food Fraud Prevention ACADEMY

ISO 27000 TITLE/ 27032 Definitions

ISO 27000/ 27001, 27032

- **Cybersecurity** or **Cyberspace security** (ISO 27031, 4.20): <u>preservation of confidentiality, integrity, and availability of information</u> in <u>the Cyberspace</u>.
- **the Cyberspace** (ISO 27031, 4.21): <u>complex environment resulting from the interaction of people, software, and services</u> on <u>the Internet</u> by means of technology devices and networks connected to it, which does not exist in any physical form
- **Internet** or **internetwork**: collection of interconnected networks
- **the Internet:** global system of inter-connected networks in the public domain
- **Internet security**: preservation of confidentiality, integrity and availability of information in the Internet
- **Virtual world**: simulated environment accessed by multiple users through an online interface

Others

- **E-commerce,** Electronic Commerce): (NIST SP 800-32) The use of network technology (especially the internet) to buy or sell goods and services.
- **B2C e-commerce** (FDA SFS E-Commerce): is the manufacturing, packaging, labeling, storage, and delivery of human and animal foods sold directly to consumers, through commercial transactions conducted electronically on the internet.
- **E-business** versus E-commerce (GAO-02-404): In a transaction-based definition, electronic commerce is restricted to buying and selling, as distinct from conducting E-business (purchasing, selling, tracking inventory, managing production, handling logistics, and supplying communications and support services).

21 © 2022 Food Fraud Prevention Think Tank LLC FoodFraudPrevention.com

21

Cybersecurity and ISO 22000 Food Safety Management

Leverage ISO 27032 Cybersecurity

22 © 2022 Food Fraud Prevention Think Tank LLC FoodFraudPrevention.com

22

Food Fraud Prevention ACADEMY

ISO 27032 Cybersecurity Guidelines

- Emphasis on collaboration (it's not just your job or just the IT department's job):
  - Information security,
  - Network security,
  - Internet security, and
  - Critical information infrastructure protection (CIIP)
    - Note: different from Critical Infrastructure Protection (CIP)
    - Note: the CIIP protection is with function specific standards such as ISO 22000 for food safety) or ISO 28000 for supply chain security.

ISO Store Order: OP-543151 | Downloaded: 2021-08-20
Single user

INTERNATIONAL STANDARD	ISO/IEC 27032

First edition
2012-07-15

Reviewed and confirmed in 2018

Information technology — Security techniques — Guidelines for cybersecurity

Technologies de l'information — Techniques de sécurité — Lignes directrices pour la cybersécurité

> You're not an expert in IT or cybersecurity
>
> and
>
> they're not an expert in food safety or the food manufacturing operations

23 © 2022 Food Fraud Prevention Think Tank LLC

FoodFraudPrevention.com

23

Food Fraud Prevention ACADEMY

NIST Prioritizing Cybersecurity Risk for Enterprise Risk Management (ERM)

NISTIR 8286B
Prioritizing Cybersecurity Risk for Enterprise Risk Management

Stephen Quinn
Nahla Ivy
Matthew Barrett
Greg Witte
R. K. Gardner

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8286B

- Prioritize vs. the 'risk tolerance'
- Food Safety: Identify the risks/ impact/ exposure
- A template to list the CIP concerns

Notional Cybersecurity Risk Register

ID	Priority	Risk Description	Risk Category	Current Assessment			Risk Response Type	Risk Response Cost	Risk Response Description	Risk Owner	Status
				Likelihood	Impact	Exposure Rating					
1											
2											
3											
4											
5											

Continually Communicate, Learn, and Update

Figure 4: Notional Cybersecurity Risk Register Template

NIST, National Institute of Standards and Technology (2021). Identifying and Estimating Cybersecurity Risk for Enterprise Risk Management (NISTIR 8286A), Internal Report Series, US Department of Commerce, [Accessed January 15, 2022], URL: https://doi.org/10.6028/NIST.IR.8286A

24 © 2022 Food Fraud Prevention Think Tank LLC

FoodFraudPrevention.com

24

Application from Food Safety Summit 2022, Cybersecurity Workshop Part1 – Roundtable Workshop

This is a summary of the Group2 discussion. This is a summary of the results from the Group 2, roundtable workshop brainstorming. This conducted at the Food Safety Summit in 2022 within the Cybersecurity Workshop series. Part 1 was an overview and introduction to the topic. Part 2 was conducted to gather insight on concerns and applications.

25

© 2022 Food Fraud Prevention Think Tank LLC

FoodFraudPrevention.com

25

Food Fraud Prevention ACADEMY

Overview and Immediate Steps

1. A recommendation to quantify the risk in terms of the food safety management accountably such as Food Safety Management System compliance or food laws and regulations (e.g., classify concerns as a possible "hazard that requires a preventive control," "failed an audit," or above the "ERM/ COSO" risk tolerance.
   - Application: You are accountable for making sure the other systems are ok. "I'm worried about the compliance of 'x' for what I am accountable for." E.g., ask "there is this new law that I feel will impact my compliance area, but it appears outside my area of responsibility, so how are we addressing it? (don't offer but "is it my responsibility?")
2. Request an IT an audit of your people and systems – which will, if only, emphasize to your team that you are serious about this.
3. To list specific food safety concerns, consider using the NIST/ ERM Notational Cybersecurity Risk Register Template (complete the columns identified in the red box).

26

© 2022 Food Fraud Prevention Think Tank LLC

FoodFraudPrevention.com

26

Food Fraud Prevention ACADEMY

Summary Notes from the Workshop

1. Steps to review food safety system vulnerability from cybersecurity
   - Create a map of the manufacturing operations steps including pre-requisite or receiving steps.
   - On that map, identify the systems or steps that are IT-intensive or automated systems.
   - Note systems that have redundant checks (e.g., refrigeration systems that have an automated text message alert and also periodic manual temperature checks – if the automates system fails then the manual system will identify the anomaly).
   - Review IT/ automation/ cyber/ information network incidents, system weaknesses, or concerns, etc.
2. Confirm with the corporate IT team controls such as: critical IT system access controls, oversight, logging of changes, notification of changes, external access, password allocation, networked to other IT systems (customers/ suppliers), remote access/ employee (VPN Wi-Fi), remote devices (cell phones, etc. – asset tracking for everything), etc.
3. Review or recommend cross functional supplier audits that include IT and cybersecurity in addition to food safety, quality, credit, accounting, etc.
4. Review and possibly connect the food safety/ cybersecurity processes with other currently implemented monitoring systems such as quality management (e.g., moisture level, or other variables) and food defense plans, etc.

27 © 2022 Food Fraud Prevention Think Tank LLC   FoodFraudPrevention.com

27

Call to Action

28 © 2022 Food Fraud Prevention Think Tank LLC   FoodFraudPrevention.com

28

Food Fraud Prevention ACADEMY

Hazard Identification, Risk Assessment and Risk Communication

- Apply common risk management practices that are based on ISO 9000 Quality Management, ISO 31000 Risk Management, and ISO 22000 Food Safety Management.
  - ISO 9000 and ISO 31000 are foundations for food safety Hazard Analysis and Critical Control Point Plans – HACCP).
  - ISO 22000 is a foundation for the Global Food Safety Initiative (GFSI) benchmark applies to food safety management systems (FSMS) such as BRC, IFS, SQF, FSSC 22000, and others.
- Identify the food safety or food manufacturing related system weaknesses for cybersecurity
- Consider the risk assessment of issues that apply to food safety or food quality issues.
  - Focus on issues that could be a "hazard that creates a preventive control" (e.g., FSMA, FD&C Act) or a FSMA audit non-conformity (e.g., non-compliance or fail an audit)
- Present the concerns in terms of the enterprise-wide risk tolerance.
  - Expand from "cybersecurity" as a general consideration to specific types of hazards (e.g., old computers that cannot load the latest anti-virus software, automated metal detector that does not have a manual duplicate review, automate temperature control ovens, etc.)
  - Consider using the ERM/COSO "initial screening" method for assessment.

29   © 2022 Food Fraud Prevention Think Tank LLC   FoodFraudPrevention.com

29

Food Fraud Prevention ACADEMY

Call to Action
Cybersecurity and the Role of Food Safety Mangers

- The Key is "accountable" versus "responsible."
  - Accountable: you are to confirm your company meets ISO 22000
  - Accountable: for explaining to IT/ Cyber your Critical Information Infrastructure Protection (CIIP) and Critical Infrastructure Protection (CIP)
  - Not Responsible: selecting and implementing the processes across the entire enterprise – this leads to a harmonized and coordinated approach that levels the enterprise-wide risk tolerance (this is the IT/ Cybersecurity role)
  - Responsible: that your team follows the IT/ cyber requirements such as updates and registering all ICT equipment.
- **Conclusion for a Food Safety Manger (From NIST, ISO 27000, ISO 27032):**
- **You are NOT accountable or responsible for conducting IT/ cybersecurity assessments or selecting/ implementing/ managing those systems.**
- **You ARE accountable for sharing your expert, functional-area insight on critical infrastructure protection (what processes are the most vulnerable, and why) – AND assuring your system are covered.**
- **You ARE accountable to make sure you are meeting the FSMA and GFSI requirements for considering all hazards including those of cybersecurity and e-commerce.**

30   © 2022 Food Fraud Prevention Think Tank LLC   FoodFraudPrevention.com

30

Food Fraud Prevention ACADEMY

Discussion

John Spink, PhD

John.Spink@FoodFraudPreventionThinkTankLLC.com

SpinkJ@msu.edu

Twitter: Food Fraud and #FoodFraud

www.FoodFraudPrevention.com

Please review and comment on the chapter-section in the shared Google Document:

FoodFraudPrevention.com   Twitter: @FoodFraud   #FoodFraud

31

Food Fraud Prevention ACADEMY

Acknowledgements

32   © 2022 Food Fraud Prevention Think Tank LLC   FoodFraudPrevention.com

32