COLD CHAIN CONNECT

Webinars for Cold Chain Professionals

FOOD & CYBER CRIME: A GROWING THREAT TO THE COLD CHAIN?

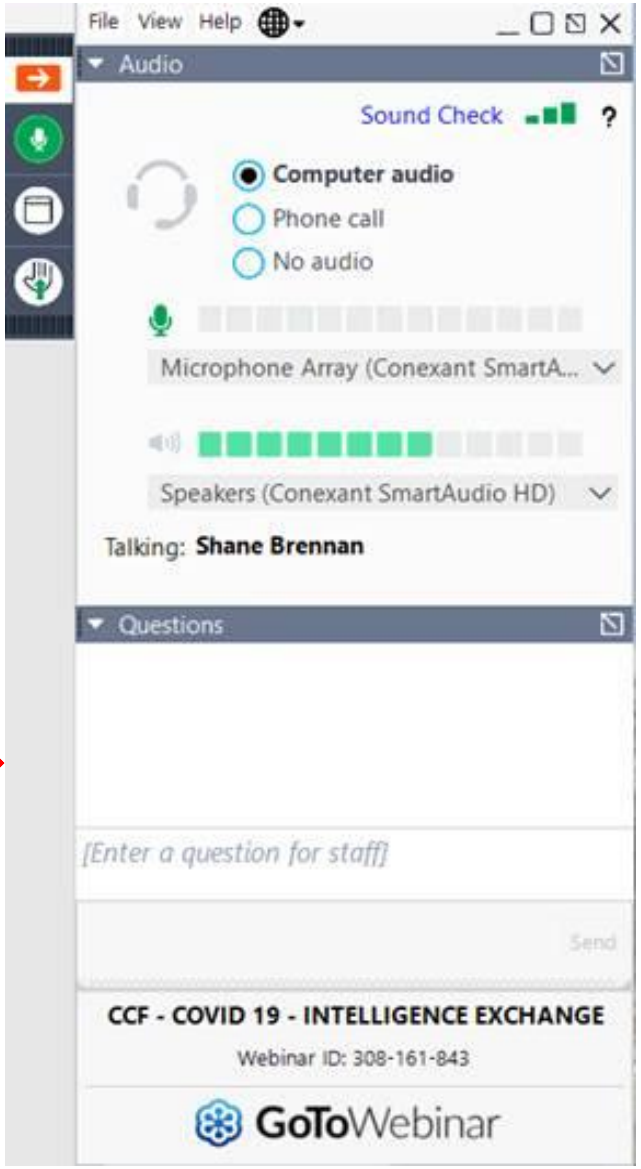
STARTING AT 12:30PM

COLD CHAIN CONNECT

Webinars for Cold Chain Professionals

FOOD & CYBER CRIME: A GROWING THREAT TO THE COLD CHAIN?

INTRODUCTION



● Computer audio
○ Phone call
○ No audio

Microphone Array (Conexant SmartA...

Speakers (Conexant SmartAudio HD)

Talking: **Shane Brennan**

[Enter a question for staff]

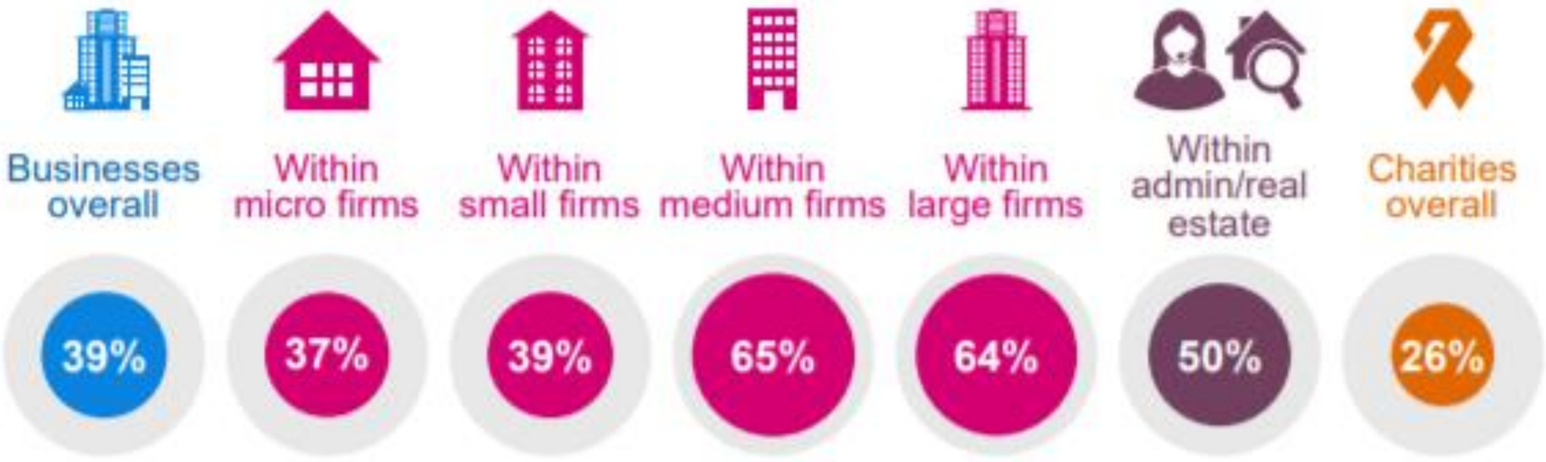
CCF - COVID 19 - INTELLIGENCE EXCHANGE

Webinar ID: 308-161-843

GoToWebinar

CYBER CRIME

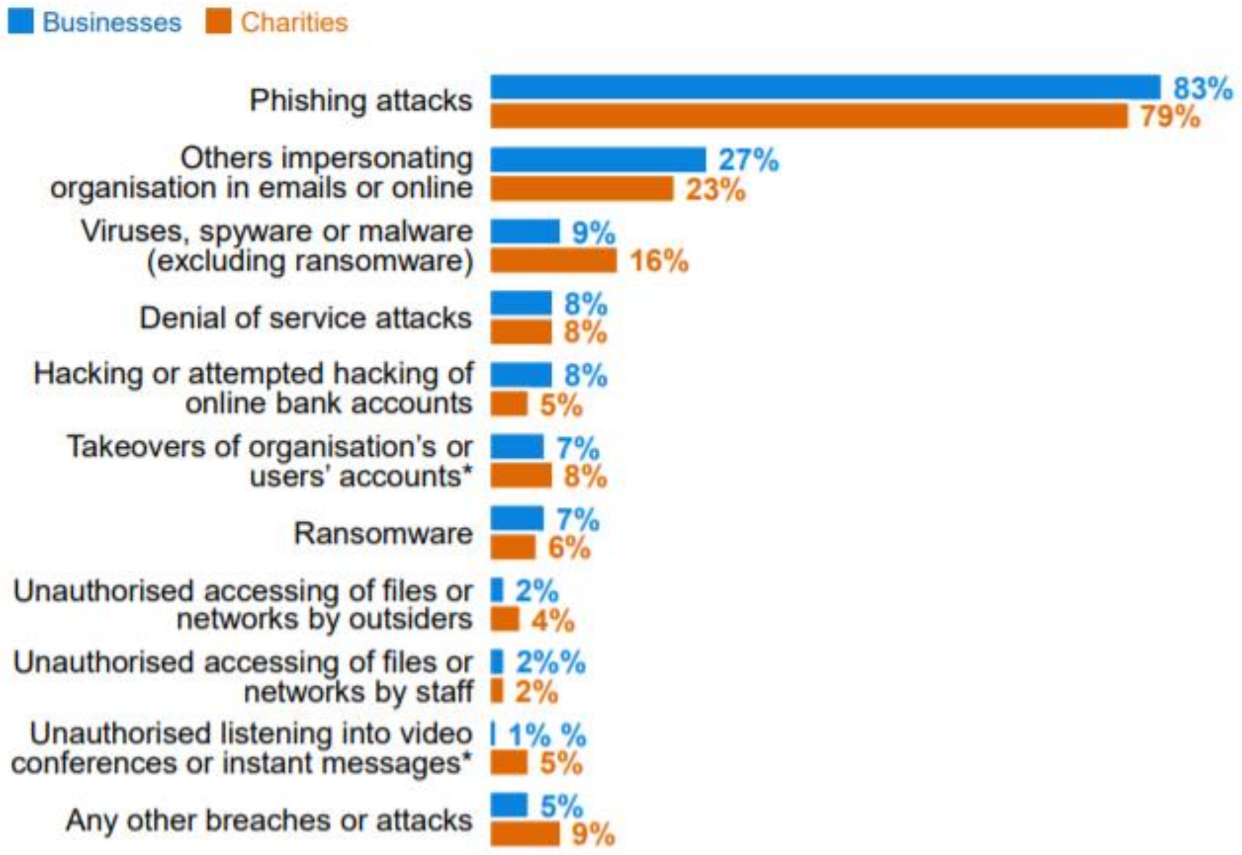
HOW COMMON IS CYBER CRIME?



Businesses overall	Within micro firms	Within small firms	Within medium firms	Within large firms	Within admin/real estate	Charities overall
39%	37%	39%	65%	64%	50%	26%

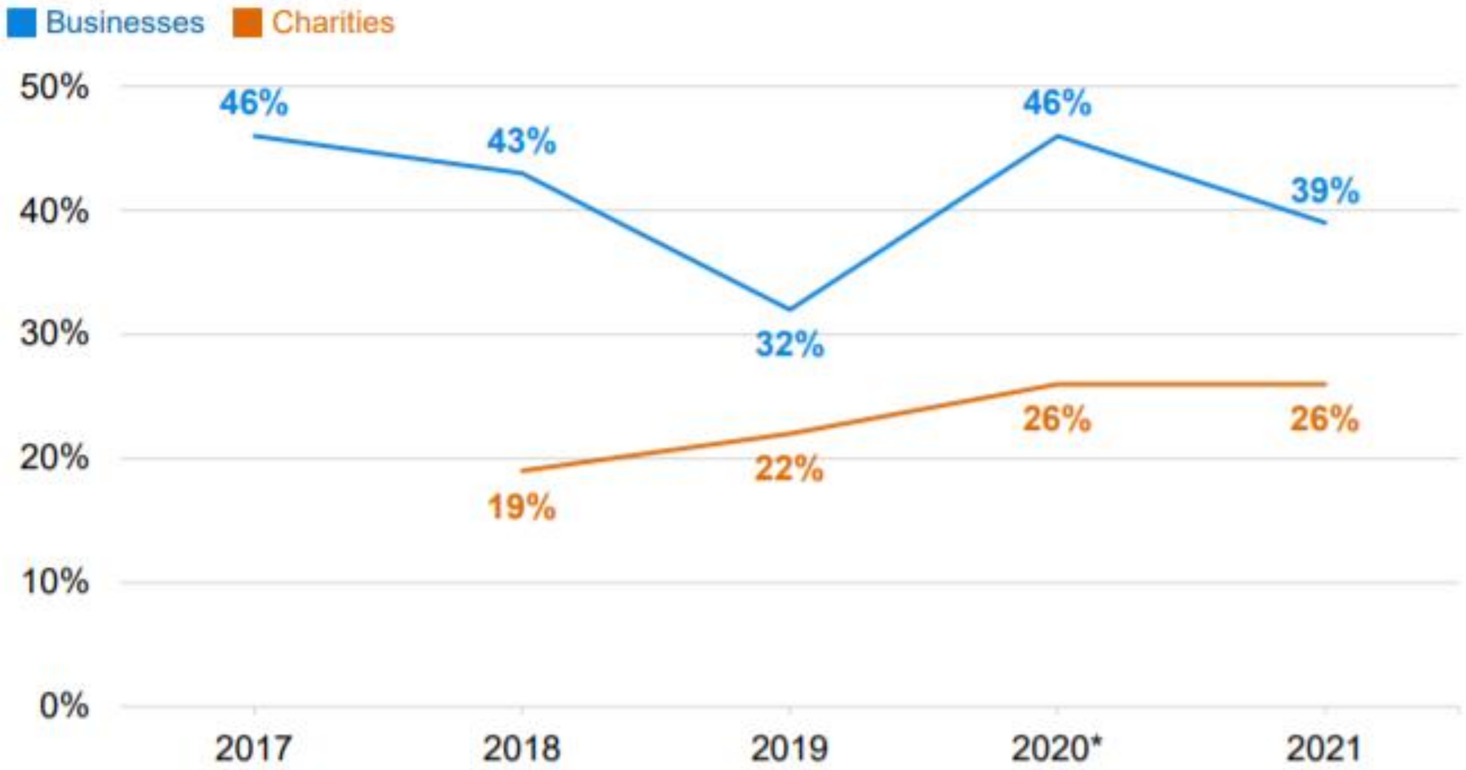
Source: Cyber Security Breaches Survey 2021, UK GOV

TYPES OF ATTACK



Source: Cyber Security Breaches Survey 2021, UK GOV

ANNUAL TRENDS



Bases: 1,000+ UK businesses per year; 300+ charities per year
*N.B. the weighting approach for businesses was changed for 2020, although this is expected to have a negligible impact on comparability to previous years. Full details of the change are available in the technical annex.

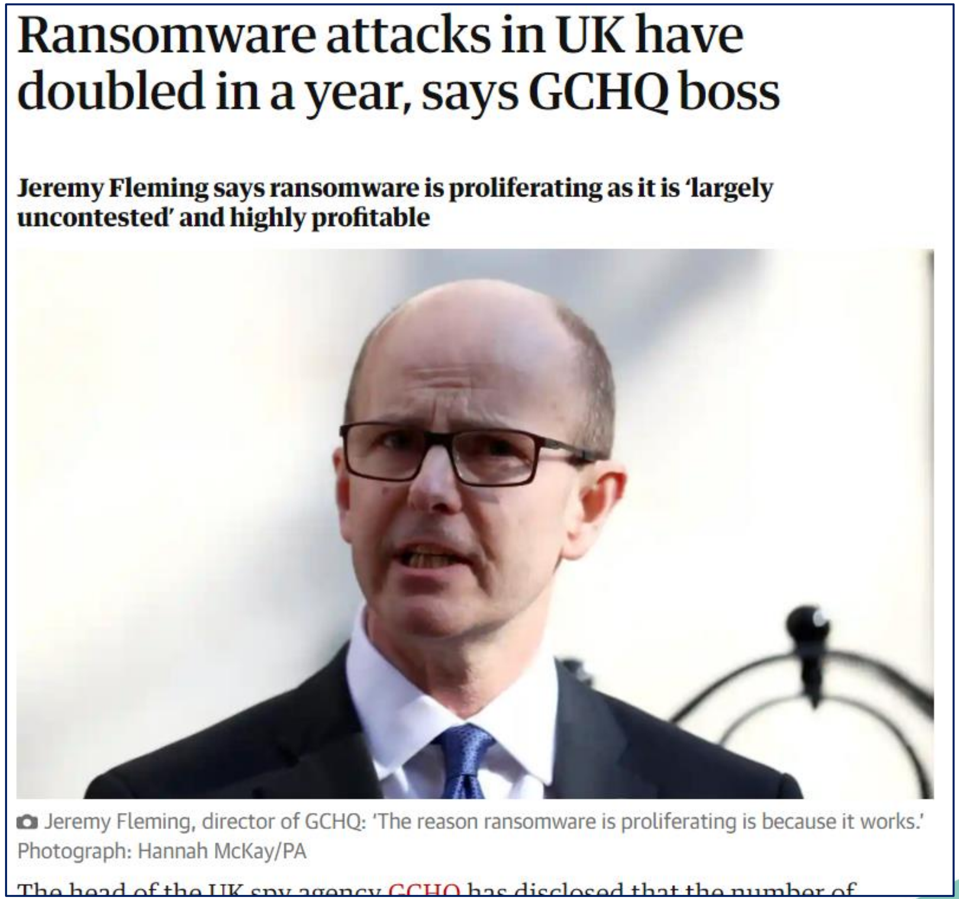
Source: Cyber Security Breaches Survey 2021, UK GOV

THE RISING THREAT……

NCSC Annual Review 2021: Ransomware became the most significant cyber threat facing the UK this year. Due to the likely impact of a successful attack on essential services or critical national infrastructure.

- Ransomware threat of leaking stolen data is almost certain to grow. Further UK victims of this dual-crime are highly likely.

- Supply chain incidents highlight the viability, effectiveness and global reach of supply chain operations as a means of compromising comparatively well defended targets. Further such operations are almost certain over the next 12 months.



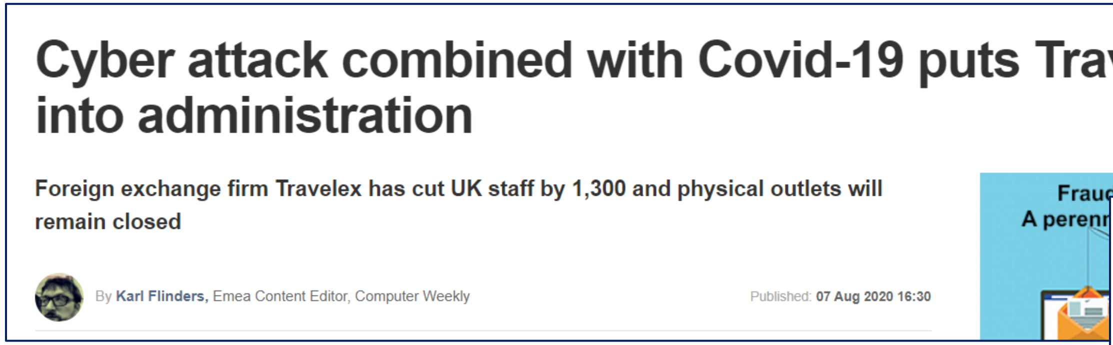
Ransomware attacks in UK have doubled in a year, says GCHQ boss

Jeremy Fleming says ransomware is proliferating as it is 'largely uncontested' and highly profitable

Jeremy Fleming, director of GCHQ: 'The reason ransomware is proliferating is because it works.' Photograph: Hannah McKay/PA

The head of the UK spy agency GCHQ has disclosed that the number of

HIGH PROFILE INCIDENTS

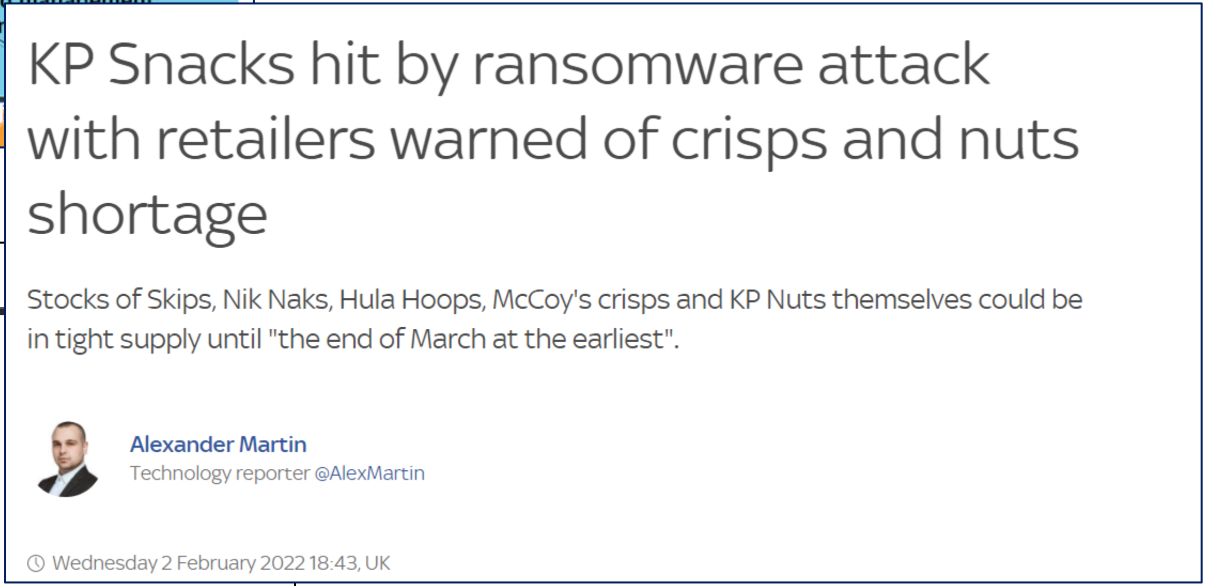


Cyber attack combined with Covid-19 puts Travelex into administration

Foreign exchange firm Travelex has cut UK staff by 1,300 and physical outlets will remain closed

By **Karl Flinders**, Emea Content Editor, Computer Weekly

Published: **07 Aug 2020 16:30**

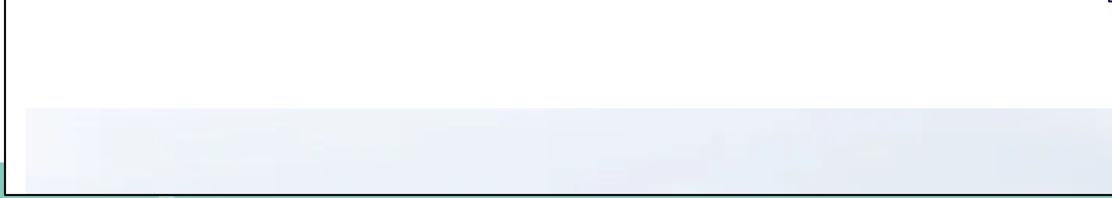


KP Snacks hit by ransomware attack with retailers warned of crisps and nuts shortage

Stocks of Skips, Nik Naks, Hula Hoops, McCoy's crisps and KP Nuts themselves could be in tight supply until "the end of March at the earliest".

Alexander Martin
Technology reporter @AlexMartin

Wednesday 2 February 2022 18:43, UK

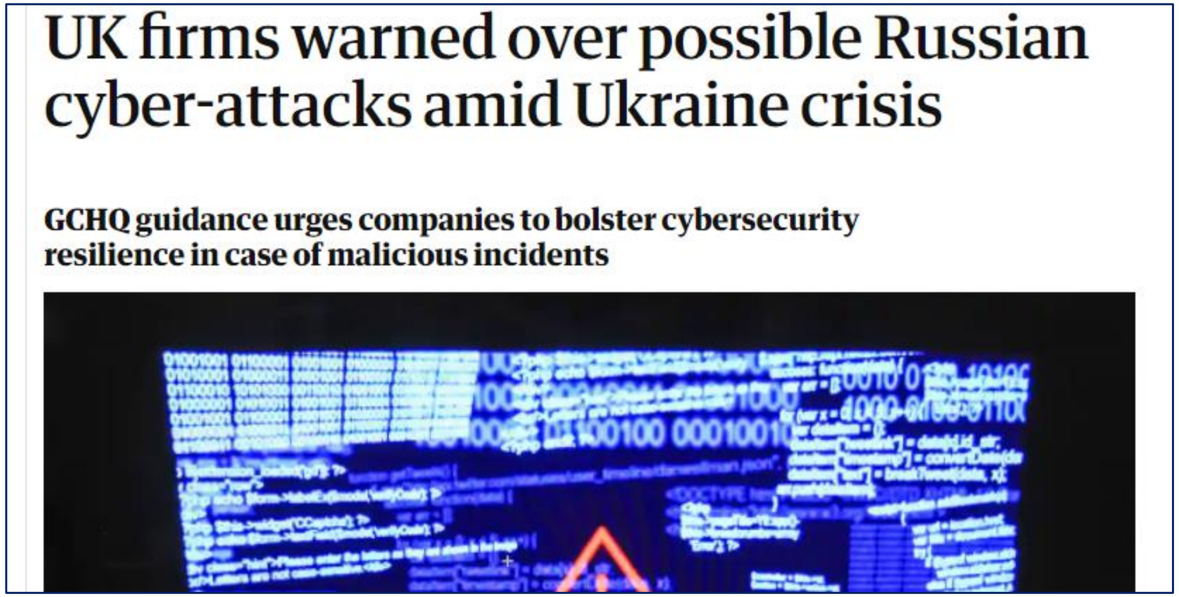


THE COST OF A MALWARE INFEC
FOR MAERSK, $300 MILLION

Nate Lord
Last Updated: Friday August 7, 2020

WHY IS THE RISK OF RANSOMWARE GROWING?

- More connected systems
- State sponsored sophistication and geopolitics
- Home working making security much harder (user monitoring)
- Profitability



UK firms warned over possible Russian cyber-attacks amid Ukraine crisis

GCHQ guidance urges companies to bolster cybersecurity resilience in case of malicious incidents

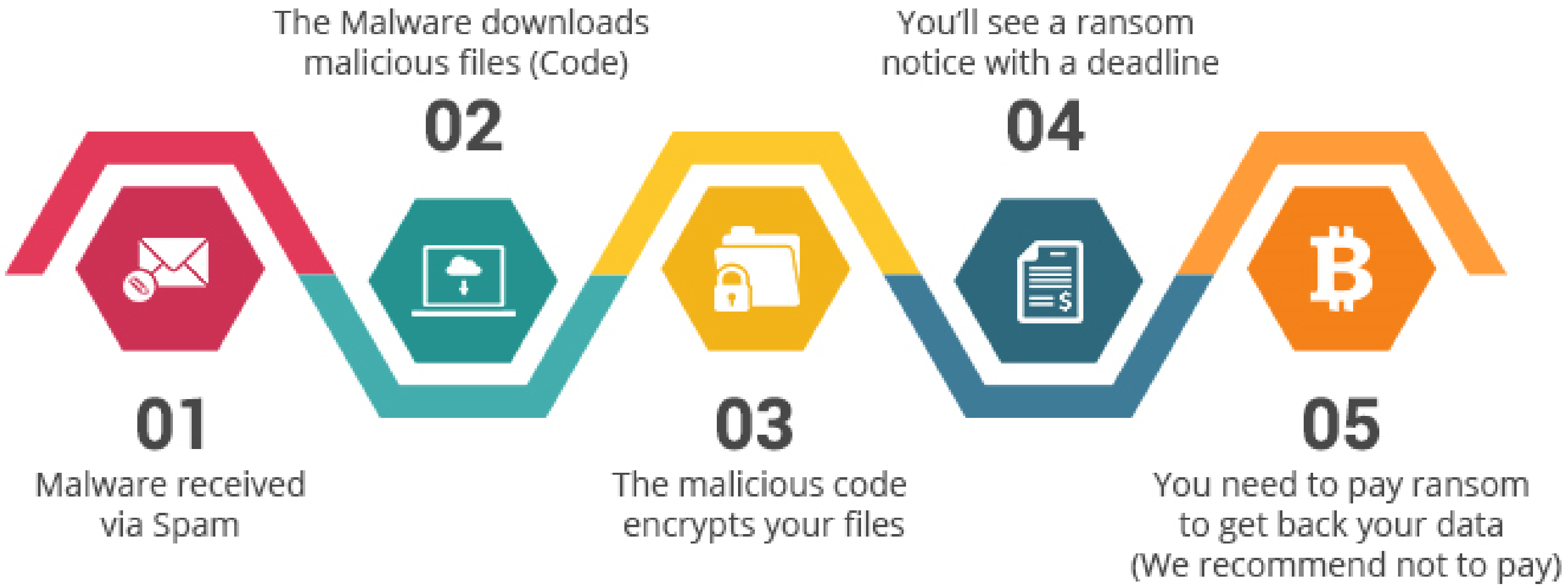
IMPACTS TO A COLD CHAIN BUSINESS

- Business paralysis: loss of WMS, customer order system etc.
- Labour time to resolve
- Downtime & lost business
- Reputation with suppliers
- Loss of sensitive material
- The ransom...
- What about cyber liability insurance?

"After ransomware struck their company, 77 percent of full-time employees temporarily lost access to networks or systems, and **26 percent couldn't fully perform their professional duties for at least a week**".

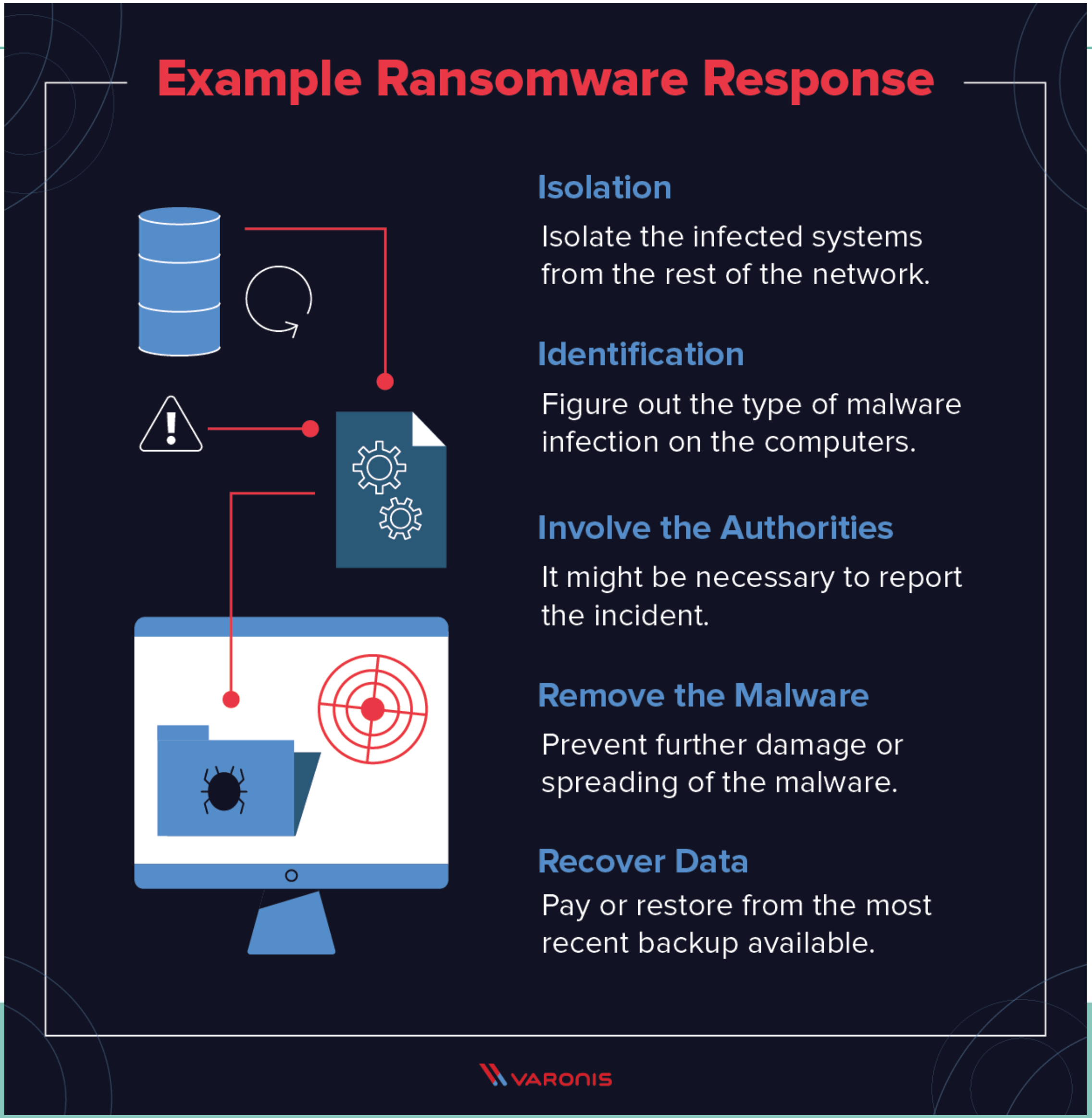
2021 Ransomware Impact Report from Keeper Security.

HOW RANSOMWARE WORKS


The Malware downloads malicious files (Code)
02
You'll see a ransom notice with a deadline
04
01
Malware received via Spam
03
The malicious code encrypts your files
05
You need to pay ransom to get back your data (We recommend not to pay)

- ‘Double extortion,’ where ransomware encrypts your data and forces you to pay a ransom to get it back and then sends your data to the threat actor, who threatens to release your sensitive data unless further ransom is paid.

A TYPICAL RANSOMWARE RESPONSE



Example Ransomware Response

Isolation

Isolate the infected systems from the rest of the network.

Identification

Figure out the type of malware infection on the computers.

Involve the Authorities

It might be necessary to report the incident.

Remove the Malware

Prevent further damage or spreading of the malware.

Recover Data

Pay or restore from the most recent backup available.

VARONIS

HOW TO PROTECT YOUR BUSINESS

PROTECTION & DATA RECOVERY PLAN

- ➢ Preparation: threat analysis
- ➢ System updates: server & user
- ➢ Educate staff to spot scams
- ➢ Security & support: anti virus and firewall
- ➢ Robust support system
- ➢ Back up: offline!
- ➢ Make a Board level responsibility
- ➢ Standards

"MAKE THEM LOOK ELSEWHERE"

National Cyber Security Centre
a part of GCHQ

NCSC Gateway to Ransomware Guidance

2 key messages to help prepare for and protect against Ransomware attacks

Backups Messaging

What would you do if your business files were lost to ransomware?

To get back up and running we recommend Offline Backups, this will enable quick restoration of business functions.
Good backups make getting back to business quicker with less long term impact.
In addition to encrypting files on your computers ransomware attacker attackers will often attempt to corrupt or alter existing backups.

Offline backups are your best defence and will mean encrypted devices can be wiped and restored from Offline backups.
Offline backups (cloud or disconnect physical media) are when the data can be protected from accidental or malicious deletion, they also should offer version retrieval. If you lose access to your files due to ransomware you should protect against this by recovering from an earlier version if a backup has been completed since the attack and preventing deletion of backups.

We recommend that you follow blog on offline backups Offline Backups

Remote Desktop Protocol (RDP) Messaging

RDP account compromise is the source of 50% of ransomware attacks.

We suggest you turn off RDP. In order to do that you need to understand *if you have it*.
NCSC's Early Warning service will help you know and provide many other benefits.
Early Warning
If you identify RDP and didn't know it was on turn it off.
If you have to use RDP we recommend using Multi-Factor Authentication and following the below guidance
MFA Guidance

Make sure you follow the principles of Privileged Access Management (PAM)" PAM Blog

Make sure that the accounts that are allowed to use it have unique passwords - try #3randomwords Three Random Words

GUIDANCE & SUPPORT: https://www.ncsc.gov.uk/

- Early Warning - Helps organisations investigate cyber attacks on their network by notifying them of malicious activity that has been detected in information feeds
- Mitigating malware and ransomware attacks – This guidance helps private and public sector organisations deal with the effects of malware (which includes ransomware).
- Cyber Security for small organisations – Cyber security advice for businesses with up to 250 employees. S*pecific SME advice and guidance is also covered in more detail below.*
- Incident management – How to effectively detect, respond to and resolve cyber incidents.
- Cyber Aware – Cyber Aware is the government's advice on how to stay secure online. It outlines six actions to take to improve your cyber security and offers a tailored plan for you or your business.
- Small Business Guide – Explains how to improve your cyber security; affordable, actionable advice for organisations.
- Top Tips for Staff & Cyber Security for Small Organisations E-learning - Cyber Security for Small Organisations and Top Tips for Staff are both designed to be integrated into your organisation's training platform or can simply be accessed via our website.
- Exercise in a Box - A free online tool which helps organisations find out how resilient they are to cyber attacks and practise their response in a safe environment. Exercises include from 15-minute micro exercises, 1-3 hour discussion based exercises and a 3-4 hour simulation exercise.

GUIDANCE & SUPPORT: https://www.ncsc.gov.uk/

- Response & Recovery Guide - Guidance that helps organisations prepare their response to and plan their recovery from a cyber incident.
- Ten Steps to Cyber Security - Takes things a little further: breaks down the task of defending networks into ten essential components.
- COVID -19 Guidance – This guidance includes home working, video conferencing and moving your organisation from physical to digital
- Supply Chain Security - The guidance will provide organisations with an improved awareness of supply chain security, as well as helping to raise the baseline level of competence in this regard, through the continued adoption of good practice.
- Board Toolkit – Designed to encourage essential cyber security discussions between the Board and their technical experts.
- Cyber Essentials – Cyber Essentials government backed certification scheme helps you to guard against the most common cyber threats and demonstrate your commitment to cyber security.
- The Cyber Essentials Readiness Tool – This is a free, online resource that guides organisations through a series of questions related to the Cyber Essentials criteria to help prepare them for certification.
- Threat videos – These short videos have been produced to make the subject of ransomware, phishing and security culture easier to understand and also refers to our relevant advice.

REPORTING AN INCIDENT

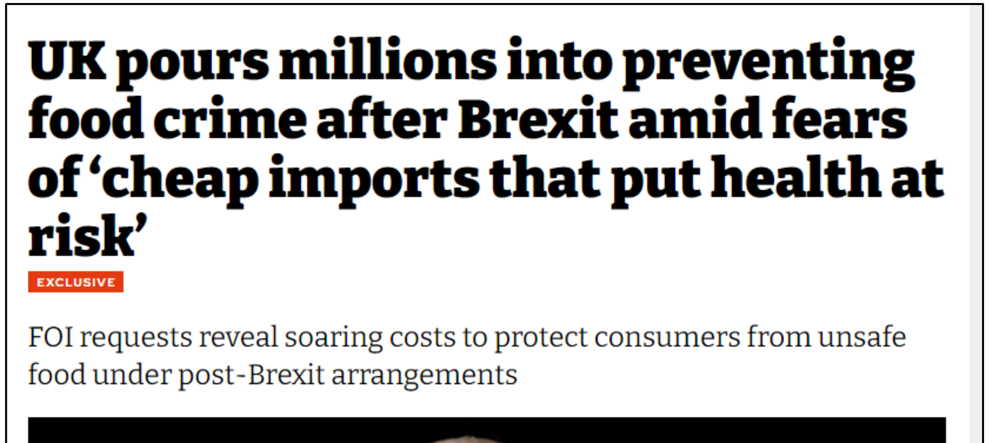
- Organisations that suffer a cyber incident or are affected by fraud should report this to Action Fraud by calling **0300 123 2040** or go to www.actionfraud.police.uk.

- In Scotland, Police Scotland's 101 call centre should be contacted.

- Cyber incident's can also be reported to the NCSC via an online form which is monitored 24/7 - https://report.ncsc.gov.uk/

FOOD CRIME & THE COLD CHAIN

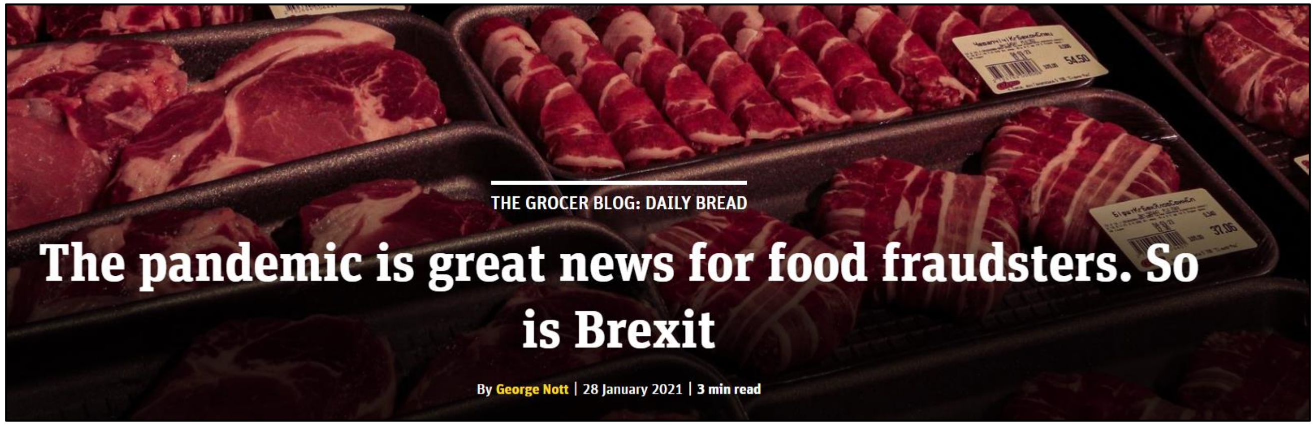
FOOD CRIME – RISING?



UK pours millions into preventing food crime after Brexit amid fears of 'cheap imports that put health at risk'

EXCLUSIVE

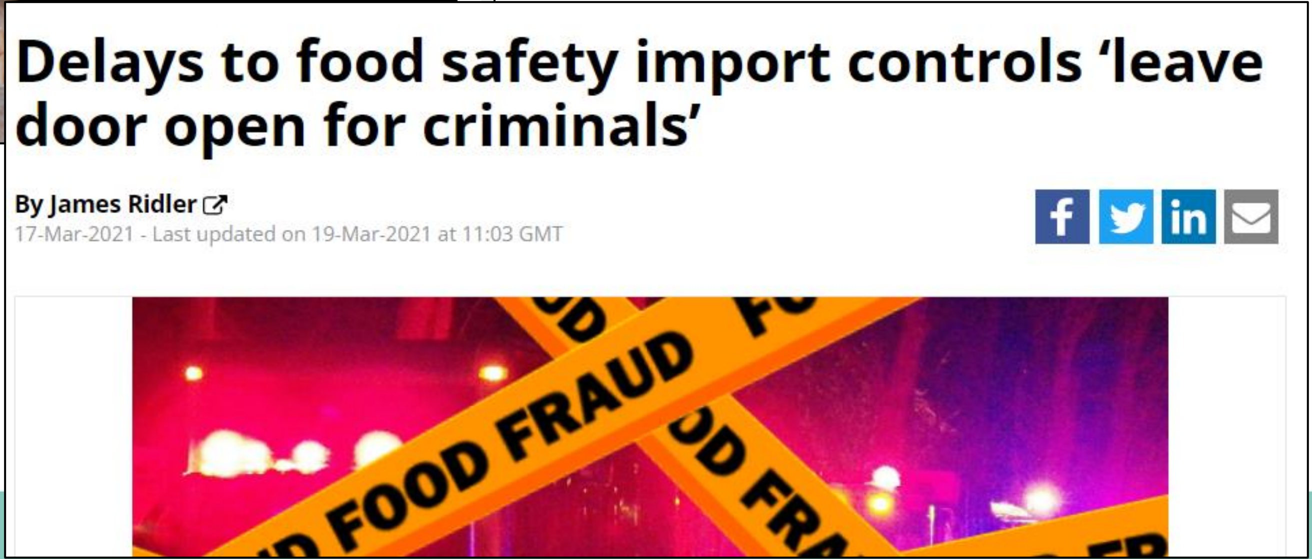
FOI requests reveal soaring costs to protect consumers from unsafe food under post-Brexit arrangements



THE GROCER BLOG: DAILY BREAD

The pandemic is great news for food fraudsters. So is Brexit

By George Nott | 28 January 2021 | 3 min read



Delays to food safety import controls 'leave door open for criminals'

By James Ridler

17-Mar-2021 - Last updated on 19-Mar-2021 at 11:03 GMT

CCF FOOD SAFETY GUIDE

CHAPTER 1: FOOD SAFETY REGULATIONS AND CERTIFICATION STANDARDS

CHAPTER 2: DRIVING MANAGEMENT COMMITMENT AND FOOD SAFETY CULTURE

CHAPTER 3: HAZARD ANALYSIS CRITICAL CONTROL POINT (HACCP) FOR THE COLD CHAIN

CHAPTER 4: SYSTEMS AND PROCESSES SUPPORTING FOOD SAFETY

CHAPTER 5: TEMPERATURE MANAGEMENT

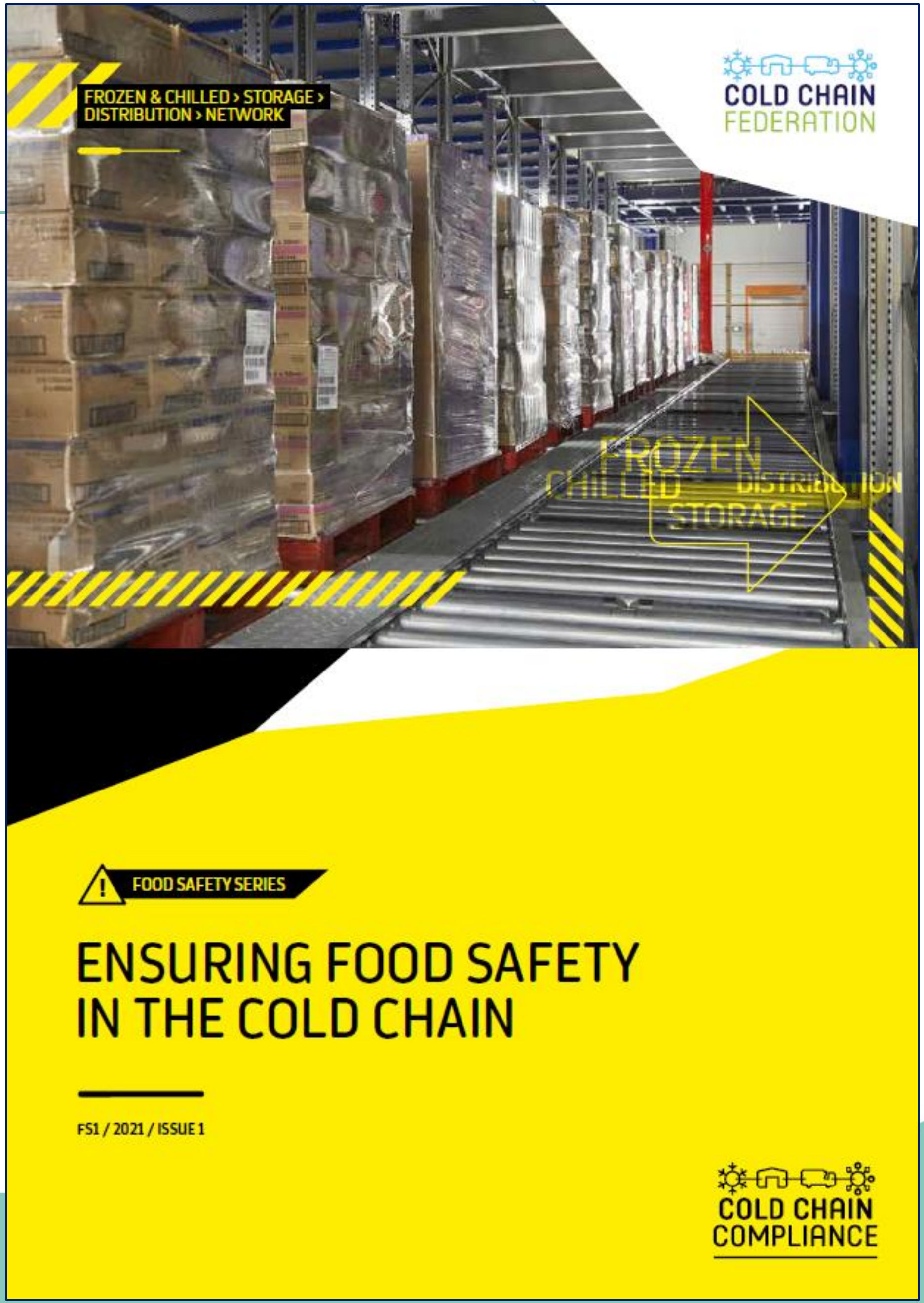
CHAPTER 6: PHYSICAL AND CHEMICAL CONTAMINATION

CHAPTER 7: FOOD ALLERGENS AND HYPERSENSITIVITY

CHAPTER 8: GOOD HYGIENE PRACTICE

CHAPTER 9: DEFENCE AGAINST FOOD CRIME IN THE COLD CHAIN

https://www.coldchainfederation.org.uk/ensuring-food-safety-in-the-cold-chain/



FROZEN & CHILLED › STORAGE › DISTRIBUTION › NETWORK

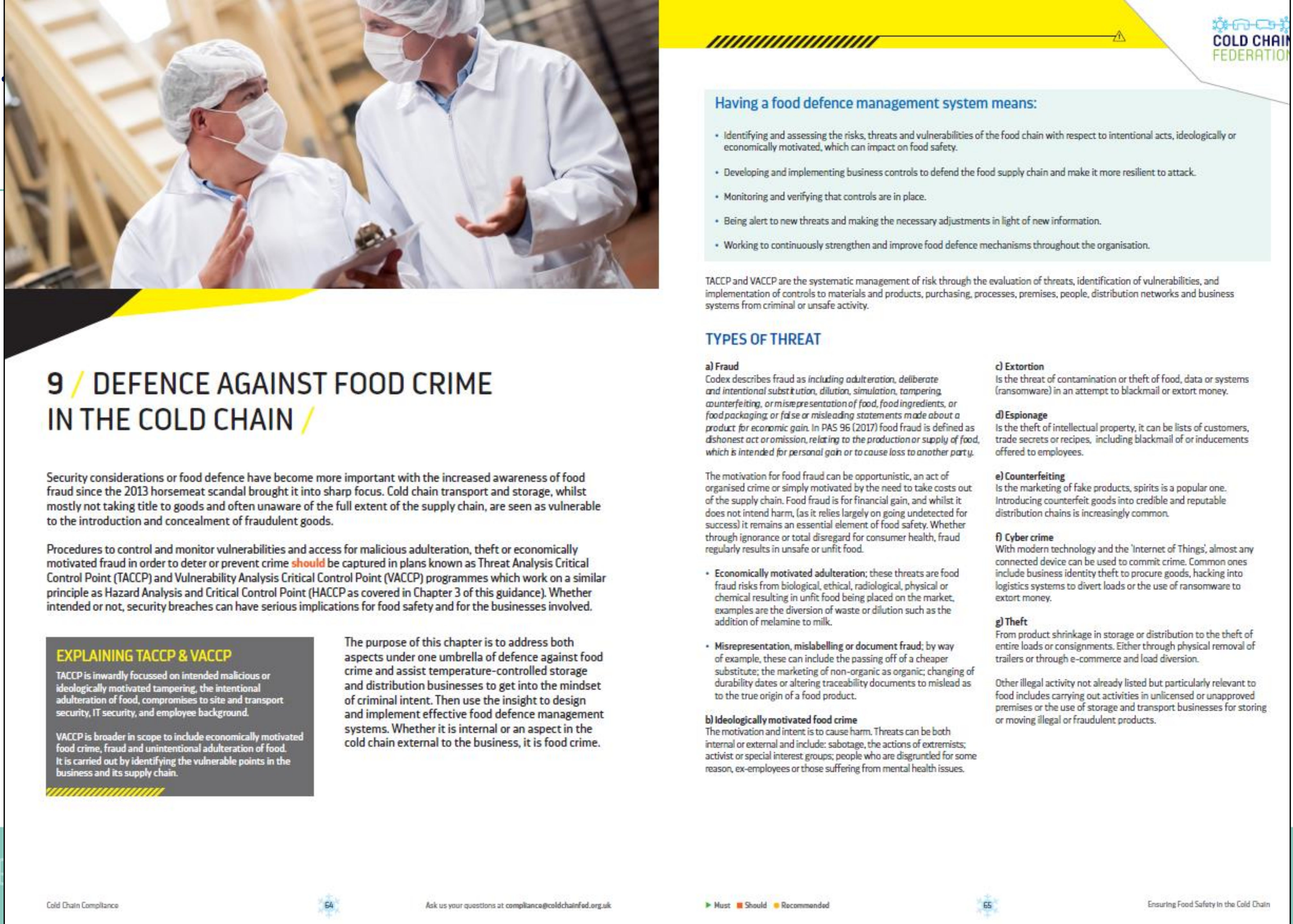
COLD CHAIN
FEDERATION

FOOD SAFETY SERIES

ENSURING FOOD SAFETY
IN THE COLD CHAIN

FS1 / 2021 / ISSUE 1

COLD CHAIN
COMPLIANCE



9 / DEFENCE AGAINST FOOD CRIME IN THE COLD CHAIN /

Security considerations or food defence have become more important with the increased awareness of food fraud since the 2013 horsemeat scandal brought it into sharp focus. Cold chain transport and storage, whilst mostly not taking title to goods and often unaware of the full extent of the supply chain, are seen as vulnerable to the introduction and concealment of fraudulent goods.

Procedures to control and monitor vulnerabilities and access for malicious adulteration, theft or economically motivated fraud in order to deter or prevent crime **should** be captured in plans known as Threat Analysis Critical Control Point (TACCP) and Vulnerability Analysis Critical Control Point (VACCP) programmes which work on a similar principle as Hazard Analysis and Critical Control Point (HACCP as covered in Chapter 3 of this guidance). Whether intended or not, security breaches can have serious implications for food safety and for the businesses involved.

EXPLAINING TACCP & VACCP

TACCP is inwardly focussed on intended malicious or ideologically motivated tampering, the intentional adulteration of food, compromises to site and transport security, IT security, and employee background.

VACCP is broader in scope to include economically motivated food crime, fraud and unintentional adulteration of food. It is carried out by identifying the vulnerable points in the business and its supply chain.

The purpose of this chapter is to address both aspects under one umbrella of defence against food crime and assist temperature-controlled storage and distribution businesses to get into the mindset of criminal intent. Then use the insight to design and implement effective food defence management systems. Whether it is internal or an aspect in the cold chain external to the business, it is food crime.

Having a food defence management system means:

- Identifying and assessing the risks, threats and vulnerabilities of the food chain with respect to intentional acts, ideologically or economically motivated, which can impact on food safety.
- Developing and implementing business controls to defend the food supply chain and make it more resilient to attack.
- Monitoring and verifying that controls are in place.
- Being alert to new threats and making the necessary adjustments in light of new information.
- Working to continuously strengthen and improve food defence mechanisms throughout the organisation.

TACCP and VACCP are the systematic management of risk through the evaluation of threats, identification of vulnerabilities, and implementation of controls to materials and products, purchasing, processes, premises, people, distribution networks and business systems from criminal or unsafe activity.

TYPES OF THREAT

a) Fraud
Codex describes fraud as *including adulteration, deliberate and intentional substitution, dilution, simulation, tampering, counterfeiting, or misrepresentation of food, food ingredients, or food packaging; or false or misleading statements made about a product for economic gain.* In PAS 96 (2017) food fraud is defined as *dishonest act or omission, relating to the production or supply of food, which is intended for personal gain or to cause loss to another party.*

The motivation for food fraud can be opportunistic, an act of organised crime or simply motivated by the need to take costs out of the supply chain. Food fraud is for financial gain, and whilst it does not intend harm, (as it relies largely on going undetected for success) it remains an essential element of food safety. Whether through ignorance or total disregard for consumer health, fraud regularly results in unsafe or unfit food.

- **Economically motivated adulteration**; these threats are food fraud risks from biological, ethical, radiological, physical or chemical resulting in unfit food being placed on the market, examples are the diversion of waste or dilution such as the addition of melamine to milk.
- **Misrepresentation, mislabelling or document fraud**; by way of example, these can include the passing off of a cheaper substitute; the marketing of non-organic as organic; changing of durability dates or altering traceability documents to mislead as to the true origin of a food product.

b) Ideologically motivated food crime
The motivation and intent is to cause harm. Threats can be both internal or external and include: sabotage, the actions of extremists; activist or special interest groups; people who are disgruntled for some reason, ex-employees or those suffering from mental health issues.

c) Extortion
Is the threat of contamination or theft of food, data or systems (ransomware) in an attempt to blackmail or extort money.

d) Espionage
Is the theft of intellectual property, it can be lists of customers, trade secrets or recipes, including blackmail of or inducements offered to employees.

e) Counterfeiting
Is the marketing of fake products, spirits is a popular one. Introducing counterfeit goods into credible and reputable distribution chains is increasingly common.

f) Cyber crime
With modern technology and the 'Internet of Things', almost any connected device can be used to commit crime. Common ones include business identity theft to procure goods, hacking into logistics systems to divert loads or the use of ransomware to extort money.

g) Theft
From product shrinkage in storage or distribution to the theft of entire loads or consignments. Either through physical removal of trailers or through e-commerce and load diversion.

Other illegal activity not already listed but particularly relevant to food includes carrying out activities in unlicensed or unapproved premises or the use of storage and transport businesses for storing or moving illegal or fraudulent products.

▶ Must ■ Should ● Recommended

TYPES OF FOOD THREAT

- Fraud
  - Economically motivated adulteration
  - Misrepresentation, mislabelling or document fraud
- Ideologically Motivated Food Crime
- Extortion (ransomware)
- Espionage
- Counterfeiting
- Theft

European Distribution Fraud

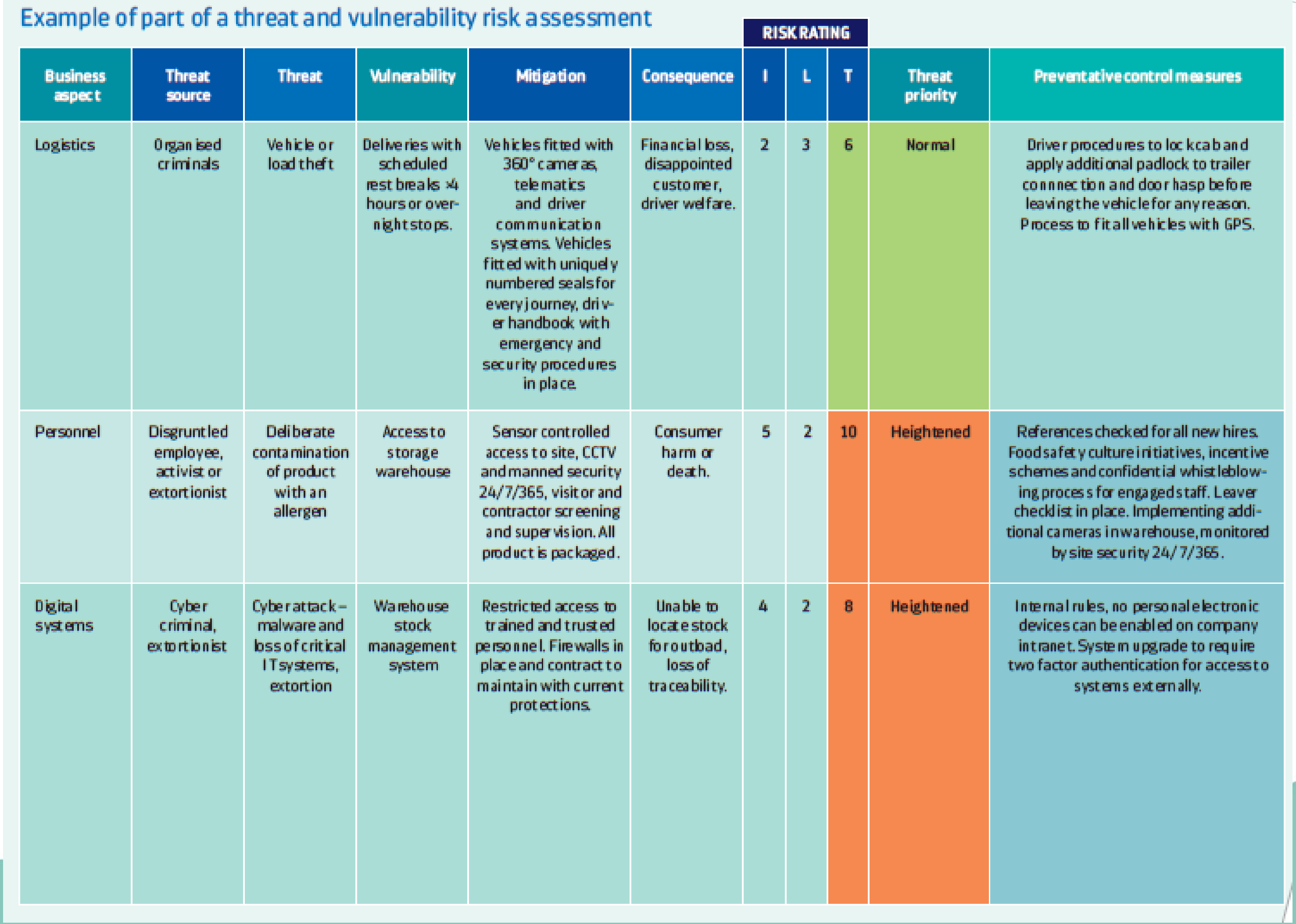
- European Distribution Fraud (EDF) is where an individual or group, imitates the details of a legitimate company, in order to pass credit checks and purchase goods.

- Once they have received the goods they cannot be contacted

- It is at this point that the victim makes contact with the legitimate company only to discover that they never actually placed the order.

WHAT CAN YOU DO

- ➢ Have a plan....
- ➢ Consider:
  - ▪ People
  - ▪ Products
  - ▪ Premises
  - ▪ Distribution
  - ▪ Business operations
- ➢ Report to NFCU:
  - ▪ 0207 276 8787
  - ▪ https://www.food.gov.uk/contactbusinessesreport-safety-concern/report-a-food-crime



Example of part of a threat and vulnerability risk assessment

						RISK RATING				
Business aspect	**Threat source**	**Threat**	**Vulnerability**	**Mitigation**	**Consequence**	**I**	**L**	**T**	**Threat priority**	**Preventative control measures**
Logistics	Organised criminals	Vehicle or load theft	Deliveries with scheduled rest breaks >4 hours or overnight stops.	Vehicles fitted with 360° cameras, telematics and driver communication systems. Vehicles fitted with uniquely numbered seals for every journey, driver handbook with emergency and security procedures in place.	Financial loss, disappointed customer, driver welfare.	2	3	6	Normal	Driver procedures to lock cab and apply additional padlock to trailer connection and door hasp before leaving the vehicle for any reason. Process to fit all vehicles with GPS.
Personnel	Disgruntled employee, activist or extortionist	Deliberate contamination of product with an allergen	Access to storage warehouse	Sensor controlled access to site, CCTV and manned security 24/7/365, visitor and contractor screening and supervision. All product is packaged.	Consumer harm or death.	5	2	10	Heightened	References checked for all new hires. Food safety culture initiatives, incentive schemes and confidential whistleblowing process for engaged staff. Leaver checklist in place. Implementing additional cameras in warehouse, monitored by site security 24/7/365.
Digital systems	Cyber criminal, extortionist	Cyber attack – malware and loss of critical IT systems, extortion	Warehouse stock management system	Restricted access to trained and trusted personnel. Firewalls in place and contract to maintain with current protections.	Unable to locate stock for outload, loss of traceability.	4	2	8	Heightened	Internal rules, no personal electronic devices can be enabled on company intranet. System upgrade to require two factor authentication for access to systems externally.

SUPPORT & GUIDANCE

Food Fraud Resilience Self-Assessment Tool:

guides food business owners and employees through a series of questions designed to help them identify the risk to their business from food crime, and outlines steps that they can take to mitigate this.

Can be found at:

https://www.food.gov.uk/food-fraud-resilience-self-assessment-tool

Food fraud resilience self-assessment tool

NFCU Newsletter

Available to all who work in the food industry

Recent updates following stakeholder feedback

To receive copies of the NFCU Industry Newsletter contact:

NFCU.Outreach@food.gov.uk

HOW CAN THE FEDERATION HELP?

- Run further events to bring members the latest information and advice.
- Work with authorities to provide warnings, guidance and help during an incident.
- Bespoke cold chain guidance
- Knowledge sharing…. a confidential partner.

COLD CHAIN FEDERATION

COLD CHAIN FEDERATION FOOD & CYBER SECURITY WEEK

17th and 18th May 2022