Cyber-Crime and Fraud Victimization of Online Halal Meat Shops: A Negative Image Propagation

Siti Nur Azizah[1]
Universitas Negeri Surabaya, Indonesia

Abstract

Halal food is a critical tenet of the Muslim religion, and the rising criminal activity in the global food supply chain is troubling. Numerous instances of contaminated meat have been discovered. Malaysia is well-known for its sensitivity to halal norms, and its prominence as an international halal centre attests to the country's thriving halal ecosystem. Food crimes, food adulteration, and fraud are wreaking havoc on the meat business and the country's status as a halal ecosystem. This study aimed to investigate the themes of fraud victims, halal food fraud, and perceptions of fraud in Malaysian food crimes. The study's findings demonstrated that food crimes could be reduced by increasing customer and company owner awareness and establishing consensus across halal agencies. The government and halal authorities must implement procedures and processes to eradicate these offences to safeguard the country's halal status. The report makes recommendations and discusses the ramifications for the industry, government agencies, and policymakers.

Keywords: halal, crime, meat cartels, fraud, online meat shops, fraud victimization.

1. Introduction

Halal food is always a priority for Muslims, as their Islamic teachings and values prefer particular norms and restrictions regulating food customization; thus, the halal concept is gaining traction in the research sector. Halal is the core emphasis of the food sector in Malaysia, covering awareness, information, traceability, certificates, processing, manufacturing, and even every little corner. It is vital to consider alternative viewpoints on halal food in the millennial era. The world is rapidly expanding due to technological breakthroughs and their application in every field; similarly, the cyber world and technology are also prevalent in the halal food industry. In the context of halal food and cyber technology, halal meat stores also leverage internet services to access the same rising consumers; nevertheless, these sources are pretty replete with crimes and scams associated with online shopping (FAN & NUNYUIE, 2019; Yucedal, 2010). Thus, the article's subject discusses the impact of cybercrime and fraud victimization in the world of online halal meat shops and

[1] Study Program of Law, Universitas Negeri Surabaya, Jl. Lidah Wetan, Surabaya 60213, Indonesia. Email: sitinurazizah@unesa.ac.id

accomplishes specific objectives, including the examination of the effects of cybercrime and fraud victimization in both positive and negative spheres, as well as the evaluation of consumer and business actors from both perspectives.

The requirements for Halal cuisine are extensively detailed in the Quran (the holy book) and Sunnah: "What is forbidden to you is that which dies of itself, and blood, and swine flesh, and that on which any other name than Allah has been invoked, and the strangled (animal) and that beaten to death, and that killed by a fall, and that killed by being smitten with the horn, and that which wild beasts have eaten, except what you slaughter, and what is sacrificed on stones set up (as idols), and that which you divide with the arrows (Al-Maedah 5:3).

Continuing with the notion of halal, which has the literary meaning of permissibility in Islam, it revolves around the food and beverage industries, whereas haram exists to indicate the ban of specific things following Islamic values and Shariah standards. Concerning halal cuisine in the cyber world, the internet, defined as a collaborative web network of computers that enables electronic employment, plays a role (Saban et al., 2002). The increased internet usage has made frauds and crimes feasible worldwide, resulting in the terms cybercrime and fraud victims being coined. There is considerable dispute about the internet's impact and influence, with cybercrime being recognized as one of the most prominent negative consequences. It is defined as an act committed while violating specific rules and defrauding individuals such as consumers, on which a stiff penalty is imposed under criminal laws. To further elaborate on the concept, it is also defined as an illegal activity carried out via computers and trespassing or manipulating its use (Saini et al., 2012; Siahaan, 2018). While fraud victimization emerged as a definition of economic crime in the cyber realm, it encompasses both organizational and individualistic victimization (Schoepfer & Piquero, 2009). Fraud is the most prevalent conduct in the cyber world, resulting in financial loss and violations of religious beliefs, so casting a poor light on the cyber world. Online shopping is popular because it allows convenience at home, and cybercrime reports have reached 450 USD billion. Therefore, it is critical to focus on cybercrime and victimization awareness to develop a holistic strategy for online buying. As a result, a cyberwar has erupted, posing a threat to the industrial and organizational sectors.

Malaysia's food business has been booming, and halal food products, in particular, have become a market phenomenon. The rapid expansion of hygiene and food safety legislation contributes to the market's growth. However, recent examples of food fraud involving the processing and packing of food reveal a connection between food fraud and organized crime within the food supply chain. Most food crimes involve the misuse of the halal food brand and status. In 2020, Malaysian authorities seized 1500 tonnes of illegal meat from a cartel transporting meat from Ukraine, Brazil, China, and Argentina (Ariffin et al., 2021). The organization's presence revealed widespread fraud and crime throughout the country's beef supply chain. Thus, the current study delves into these issues. The study's primary objective is to assess the impact of cybercrime and online food fraud on the Malaysian meat industry, ascertain consumers' and producers' perceptions of syndicates and cartels pushing non-halal

products in the markets, and examine the industry's security measures. The report will reflect on current findings of the prevalence of supply chain issues and emphasize the authorities' probationary actions.

The remainder of the essay is structured as follows: Section 2 discusses the literature review, Section 3 discusses the research methodology, Section 4 discusses the findings, and Sections 5 and 6 examine the study's conclusion and implications.

2. Literature review

2.1 Halal food

Halal is a term that Muslims refer to their Islamic ideals and lifestyle standards. It is concerned with food, beverages, and the wearing of clothing, among other things. When it comes to food, halal is one of the primary considerations for Muslims, particularly in their preparation, manufacturing, processing, and other procedures to ensure that halal ingredients and methods are used to prepare this meal. Globally, the halal market accounts for around 20% of the food sector, and it is estimated that the halal market will grow by 75% within the next thirty years. Thus, the meat business contributes to the global halal market for Muslim consumers, where halal meat refers to the meat of animals considered permissible for slaughter in Islam and their halal manufacture. According to available data, halal food fraud is receiving increased attention now that the industry of halal supply chains is investing heavily and providing an extensive service. It is hoped to determine whether these halal food supply chains are legitimate or fraudulent, as generally observed cases revealed the fraud of halal food supply chains by investing in food frauds. The 352 respondents' data showed that Muslim consumers' awareness and perceptions of halal food fraud are significantly related to their education, age, gender, and occupation. In contrast, the factors associated with halal food fraud include the halal logo, labelling, packaging, authority exposure, enforcement, and consumer attitude toward the chain is pervasively influential (Ruslan et al., 2018). As a result, tremendous effort is required to educate people about halal food and legitimate supply chains, either through online resources or actual seminars.

Food fraud is defined as the purposeful or intentional substitution, addition, or terming of food or packaging or labelling of food to maximize profit in the food industry (Spink & Moyer, 2011). In halal food fraud, it is visible that producers and manufacturers include non-halal food products or ingredients that do not adhere to Islamic shariah. Additionally, halal food fraud includes substituting valuable food ingredients and adding low-cost, low-quality products, making it fraudulent (Jaswir et al., 2017). Globally, non-Muslim countries such as Brazil, Australia, India, France, China, the Netherlands, and Spain supply halal meat. As a result, the concept of halal is gaining traction among Muslim customers. According to reports, contamination of halal meat products rendered them unfit for consumption by Muslims. For example, such a case was reported in Malaysia, where frozen meat of halal and non-halal categories was stored together, creating confusion when supplied at the Port of Tanjung Pelepas (Said, 2017).

The presence of even the tiniest amount of non-Halal ingredients will invalidate

the Halal designation, demonstrating the sensitivity and criticality of the Halal meat supply chain (Ab Talib et al., 2015). Kadir et al. classified the Halal poultry meat supply chain into three distinct processes: pre-slaughter, slaughter, and post-slaughter (Abd Kadir et al., 2016). The same argument might be used to address the various challenges encountered in the Halal meat supply chain. Similarly, meat adulteration occurs through mislabeling the logo and components (Montowska & Pospiech, 2010). In contrast to this, it is always observed that verifying the halal status of food is difficult when the product is processed and packed (Zakaria, 2008). Meat supplies available via the internet, such as online services offering halal meat in Malaysia, should be checked for potential criminal activity and fraud in rendering and catering to the issues.

2.2 Cybercrime

Enlightening the facts concerning cybercrime and fraud victimization, many studies have previously revealed that both terms are substantially interwoven with their minute viewpoints on internet employment. Rather than accurately reflecting the world, defining cybercrime as a dishonest and malevolent act committed via online or internet sources or e-enabled activity breaches norms and requirements (Burden & Palmer, 2003). This term cannot be defined solely in criminal terms. However, it must include hacking, vandalism, virus dissemination, service attacks, hijacking, baking misuse of the internet, identity or information theft, defamation, blackmailing, cyber obscenity, pornography, hate sites, money laundering, copyright infringements, encryption, and cyber-terrorism. With the advancement of technology and its use, numerous crimes involving internet affiliation have been detected; therefore, it is necessary to highlight some facts about cybercrime. For example, cracking falls under the category of cyberspace fraud and scam, in which individuals engage in certain fun activities or scamming by cracking some codes of passwords or internet web blockages. It includes both the virus and distributor categories.

Similarly, pranksters are a prevalent form of cybercrime in which particular methods and reasoning are applied to the internet domain to achieve desired objectives while posing no long-term harm. Another criminal activity over computers is hacking, which involves breaking into computer systems in educational settings, personal computers, organizational or industrial settings and extracting information for their benefit. Career criminal activity refers to earning money through crimes committed over the internet, computer, and cyberspace; at times, this results in the creation of the Mafia system; at other times, this is simply a way to earn a little and muddle through. Cyber terrorism is another type of cybercrime that refers to the criminal hacking of government entities for illicit objectives. It encompasses online trafficking when a specific purpose is attained by internet hacking to benefit a vast business. Cyberbullying is also a type of cybercrime in which abuse occurs online, such as posting, name-calling, faking profiles, and sending rude and vicious email messages that appear to be observed while inflicting damage to the original shapes. Salami attackers refer to financial attacks carried out using the internet and computer employment in which bank servers are hacked, manipulated, and other intentional infractions are committed (Sabillon et al., 2016). While discussing vandalism, it is

most likely that websites are hacked first, and then the necessary content is created to communicate with the audience, such as political motivations are vandalized via cyberspace, or company-based projects are damaged via the internet. Service attacks refer to the denial of service or blocking websites for organizational purposes via cyber-attacks.

Similarly, copyright infringement occurs when individuals steal content from other websites and claim it as their own; hijacking falls under the category of alternating companies' use via internet hijacking, continuing with the fact that encryption also exists through online internet sources to monitor internet use. Concluding the intent of crimes in cyberspace and simplifying the method, online crimes are committed in various ways, whether for personal or organizational gain. These crimes are rapidly expanding in number and gaining recognition worldwide (Burden & Palmer, 2003).

Cybercrime is often defined as the misuse of the internet and computers, including data interception, alteration, data theft, network crime, network sabotage, illegal access, and fraud and forgeries. The rise in cybercrime has been reported in the last five to ten years, with some claiming that use of the internet and computer systems increased during a pandemic, while a survey of approximately 400 respondents revealed that cybercrime had impacted them significantly. Whether victims of data theft or hacking via the internet, cyberspace is becoming unsafe for the world. As a result, the necessity to provide a safe and secure environment is prioritized (Kashif et al., 2020).

2.3 Fraud victimization

The online world's fraud victimization falls under the organizational and individualistic categories, and economic crime encompasses both organizational and individualistic victimization (Schoepfer & Piquero, 2009). Fraud is the most prevalent conduct in the cyber world, resulting in financial loss and violations of religious beliefs, so casting a poor light on the cyber world. Prior research indicates that fraud and white-collar victimization are the same internet crimes. Schoepfer and Piquero (2009) revealed that age and risk-taking behavior are predictors of fraud victimization. Online buying resources readily dupe people with adventurous tendencies, and those with a less than ideal age, for example, those of fewer ages, are also misled and defrauded by online shopping resources.

According to world studies, one-third of the American populace is victim of online retailers. It is a white-collar crime victimization that is more harmful than street crime victimization, and victims of fraudulent schemes are more traumatized than street crime victims, in part because fraudulent victims engage in self-indulgence during the scheme's activity and begin self-blaming as a result of the scam (Copes et al., 2001; Shichor et al., 2001). Thus, it can be concluded that online fraud victimization is more detrimental than traditional victimization. Although fraud is sometimes associated with white-collar crime, the two are not synonymous; fraud is defined as "deliberately deceiving the victim by promising goods, services, or other benefits that are nonexistent, unneeded, never intended to be supplied, or grossly misrepresented" (Johnson, 2004). Individualism is associated with fraud victimization. Previous research suggests that increasing awareness, education, and knowledge about victimization can help individuals avoid becoming victims of fraud.

Fraud victimization in telemarketing identifies easily duped victims and makes recommendations on preventing such scams, as responsibility and education play a role in scams (Doocy et al., 2001). As a result, victimization by deception is highly reliant on the victims' features, habits, mental abilities, and physical experience with age. It can be readily prevented by obtaining information from reputable sources about the businesses in which the consumer invests and cultivating a positive image of online retailers.

2.4 Impact of cybercrime and Fraud victimization

According to authorized sources, cyber-criminals have upped their cyber-piracy. However, fraud and theft operations are carried out via the internet and are motivated by powerful motives. White-collar crimes refer to online crimes such as fraud and theft and harming internet sources. As crimes evolved from old to advanced technologies, an internet-based stock crime enabled crooks to gain billions over the years. Making a case for cybercrime's impact on the economic domain, the offence has resulted in frauds such as transactions that have harmed businesses. According to a report from the United Kingdom, roughly seventy-four million people were exposed to cybercrime in 2010, resulting in direct financial damage. People assume that cybercrime is a commercial technique used to generate excessive money; otherwise, profitability is not involved in online disasters (Coleman, 2011). Additionally, studies assert that international financial markets are in disarray due to computer-based crimes and victimization. It has a detrimental effect on market value by allowing for a breach in the security of economic standing, causing consumers to avoid cyber risk factors affecting their financial and insurance security (Ariz, 2000; Gordon et al., 2003).

Regarding the consumer perspective, trust is essential to consider when conducting business and attracting consumers to products. This innovation of cyber-attacks has drastically altered the view by undermining consumer trust by intruding into services such as breaking the logic of the page. As visitors stay on the page for an extended period and eventually become fraudulent, their confidence in internet websites is shattered, and consumer investments in other legitimate firms are lost. According to a recent survey of online consumers, security is a top priority for businesses on the internet. However, online transactions are also not secure, as 80 percent of customers report being terminated when asked for credit card information regarding their investments, etc. E-commerce is a risky and insecure method of shopping regarding transactions, quality, and trust. Similarly, consumer perceptions of fraud are worse regarding internet shopping, as previously established. There is confidence, credibility, and financial security at stake for consumers who may fall victim to fraud and scams and incur losses, making consumers hesitant to participate in online enterprises (Saini et al., 2012).

The Indonesian perspective on cybercrime impacts states that financial loss in the hands of trouble is around 3.4 million dollars for 2.558 cases in 2007 and increased over the years to 19,4 billion dollars for 6.347 cases in 2008 and 954 billion dollars for 954 cases in 2010, according to central bank statistics. Moving forward in time, in 2014, individuals indicated that they had not been a victim of fraud using bank transactions or online resources. Consumer confidence has been severely eroded by the widespread use of the internet for online shopping throughout the world,

including the United Kingdom, Indonesia, Malaysia, Pakistan, and India, as a result of widespread reports of scams in online shopping, making it difficult to connect with genuine customers for legitimate businesses. Several studies have been conducted on this topic (Hong & Cho, 2011; Nasution et al., 2018; Smith, 2004).

In the context of online security parameters for the food industry, particularly halal meat, countries worldwide are implementing various technologies to ensure the traceability of their supply chains. Because the risk of non-halal meat is exceptionally high during the supply chain's operation, blockchain technology is being implemented to ensure the traceability of halal meat is transparent and visible and to embed Islamic dietary laws into the system (Rejeb, 2018). Consumer perception is always considered while establishing supply chain security parameters, including perceptions of healthiness, safety, and sensory characteristics (i.e., colour, tenderness, flavour, and aroma), but with strict adherence to religion. As a result, the halal status of Muslim food products is always taken into account, and security is maintained accordingly. To mitigate the risk associated with halal meat supply chains, collaboration among many partners is held, resulting in the preservation of halal food integrity. Numerous additional parameters are included, including the use of information and communication technology (ICT) for Halal transportation, such as the Global Positioning System (GPS), Radio Frequency Identification (RFID), and Internet of Things (IoT), to monitor Halal logistics activities and ensure the security of halal meat. However, no data indicates the security criteria of halal meat's online supply chains. While expressing the facts about online tools and their vulnerability, the use of technology is highly prominent in Malaysia, resulting in the prevalence of cybercrime there; thus, data obtained in such circumstances indicates that around 332 respondents to the survey were victims of cybercrime. Therefore, a necessity that should be prioritized is vigilance over online buying resources to decrease victimization and fraud and increase consumer trust and confidence in internet strengths (Tharshini et al., 2021).

3. Methodology

The methods and research for the underlying topic were undertaken by the writers of this paper using web resources for cybercrime and regulation of halal food online retailers. This was a dual-perspective study report that discussed the motivations of both the online client and the internet marketer or the targeted businesses. The study focused on the primary concerns and identified the factors contributing to fraud victimization and halal meat shop regulation in online departments and organizations, thereby establishing the cyber aspects. The study evaluates the research objectives using a mixed-methods technique. The risks recognized by cybercrime branches worldwide aided in data organization and provided vital support for the qualitative research methodologies. Qualitative approaches were used to analyze the operations of online meat shops that regulate their processes, focus on e-customers, and attempt to expose consumer and customer exploitation via the internet sources used. The method aims to elucidate the factors that contribute to fraud victimization and identify the threats encountered by dealers in the shopping era. The threats included internet purchases, the operation of e-commerce sites, and the illegal aspects associated with the growth of meat markets. Consumers were

advised to be aware of the potential dangers they confront in the consumer society and the operating processes of the stores where they acquire their goods and services (Jing et al., 2018).

The researcher studied and reported threats using content analysis of current papers and publications, and consumer threats were found. The extensive testing conducted on halal authorizes revealed the methodology approach for the research on how halal food authorities protect their rights and how secure and safe food transactions are conducted in Malaysia. It suggested that fear of victimization has increased by two in the region, with the threat of cybercrime rising in the area and the authorities' ability to minimize fraud tactics. Several threats were identified to be faced by consumers during the checkout phases and the restoration of the success of the stages in which orders are confirmed, including being tempted by unvalued offers and the software control of potential hackers and cybercriminals connecting ways through the halal meat organization via potentially harmful resources. Numerous internet study papers paved the road for minimizing the effect and influence of how cyber officials operate to destabilize the illicit efforts to devalue the system and alter the way halal food commissions are processed (Li & Liu, 2021).

Customers and customers were interviewed in fixed proportions to ascertain the rounding effects of cybercrime on their dependency on halal meat stores in Malaysia and their customer development over time. Similar cases in the United States were brought to light for further evaluation, such as those that occurred in the United States, where a famous meat shop was subjected to a cyberattack sourced through Russia for ransom. Government officials connected through policies to find a better solution and remind the Russian government to be accountable for the criminal procedures occurring in their country.

The studies find that the attacks perpetrated against nearly 60% of men and 50% of women who were victimized by the procedures of consulting online shops and their reliance on online resources resulted in consequences that needed to be evaluated and controlled by the state's measures to combat the new wave of cybercrime occurring and the impact on online shopping stores, including those that provide halal services (Lewallen, 2021). The writers conducted a study in which they analyzed the relevant interview. The research tools included some scenario-based representations of the events, which served as a foundation for the cyber security specialists to examine the case using the available resources. Some of them were by starting with a brief introduction and explaining the brief background of the research to the marketers and the ways they will help explore the topics and information. They asked them questions related to their experience and general questions about the practices of operations they followed online to cater to the cause of cybercrimes they have seen and come through. The investigation included both general and open-ended inquiries. The following table summarizes the approaches employed.

Table 1: Survey Methods and discussions

Topics	**Discussions**
Data Security aspects	Discussed through interview sessions
Data analytical reviews conducted	Online research paper revelations noted

Cyber methods discussion	Working phases of the cybercrime and control departments' research discussed
Attack types and the cyber security wings that are probing the attacks	Cybercrime control department interviews and the research paper analysis
Weak areas of the online marketplaces	Discussed through general questions from the marketers.
Features to cater for the cyber aspects	Significant aspects that were not mentioned discussed with the organizational markets
Supervision by the Malaysian government for the cyber hacking and crime field	Malaysian cybercrime departments and NASCA research.
Additional data requirements and the analysis for the food industry	Discussed in interviews
Globalization impacts the cyber crimes	Interview analysis.

The results of the authorities' interviews were covered due to additional analysis and verification using research analysis methods following confirmation from internet sources and working on issues raised by the public in general. The research objectives were identified and established in distinct phases, and the material gathered from the conducted interviews was analyzed in light of the in-depth examination of cybercrime in Malaysia and its consequences.

Additionally, an online poll was conducted to ascertain customers' attitudes about cyber fraud. The questionnaire was distributed using a purposive sampling strategy, and the instrument developed by Ruslan et al. (2018) was customized for this study. The mean score technique and simple linear regression were utilized to determine the relationship between consumer perception, authorities, enforcement, exposure, and halal food labelling and packaging. The questionnaire was distributed over social media, and data collecting took place over two months.

4. Result and Analysis

4.1 Findings from the interview and content analysis

The research and interviews elicited questions concerning the cause and effect of cyber-attacks on the most vulnerable places. According to studies, the UK and the US were among the most attacked countries in cybercrime, including Malaysia. Online websites will be suspended, but the risks of the operating system being corrupted by potent viruses injected by cybercriminals and potential attacks on customer data would increase by 60% between 2010 and 2022. (Lewallen, 2021; Li & Liu, 2021; NACSA, 2022). Financial loss and decreased customer satisfaction were significant aspects of the region's growing cybercrime epidemic. They were cited as the primary reason for disqualifying the most entertaining and verified meat shops operating online with questions about their quality and certification.

The study's findings were succinct and demonstrated how 70% of interview

respondents agreed to utilize the internet when shopping for halal meat online in Malaysia. However, the results indicated that public fear of cyber-attacks has increased, posing several alarms to individuals and organizations fighting for the cause of attacks occurring on online stores for the potential robbery and stealth of sensitive data and finances stored and restored by businesses after years of hard work to establish their businesses. The interviewers unanimously agreed that threat on online mediums is a well-understood concept that should be considered whenever individuals disclose information online for online transactions and the data processing required to conduct business with online businesses. These are some of the benefits derived from the study papers and findings from potential interviews with online shopping consumers in Malaysia and witnesses to cyber and crime victimization via internet-based shopping mediums. Additionally, the research methods revealed that most of the concerns expressed by the interviewed people online were about the monetary reasons and the goods provided to them. For marketers and sellers, the distribution and sale of the goods became a significant threat, with 43 percent of sellers encountering cyber issues at least once in their lifetime while dealing with internet sources for the distribution of halal meat. One of the threats disco identified (Rajasekharaiah et al., 2020). Data phishing was discussed as a concern of lesser consequence than the other threats faced by online halal meat firms, as it was one of the causes preventing people from trusting online sources. Data phishing attacks accounted for 34% of all cybercrime incidents in the region (Li & Liu, 2021; Putri, 2018; Zheng et al., 2018).

The respondents indicated that increasing funding for the fight against cybercrime was one approach for cybercrime control associations to control crimes and fraud occurring in online meat markets with the most prominent investors from Muslim countries and their regulation laws. Other concerns perceived by respondents were also elicited and generalized in light of cybercrime incidents reported to date in history, and several respondents indicated faulty product deliveries and incorrect information processed by the company.

The meat producers discussed their incentives for cybercrime in the context of hacking systems with the ability to harm the market awareness of websites and items through data theft, which they perceive to be the most severe kind of fraud victimization by businesses. According to reports on cybercrime incidents at meat shops throughout the world, particularly in the United States, 60% of consumer data was compromised, and it was only possible to conduct transactions in real-time and ship halal meat orders that had been prebooked, which resulted in a loss of customers who were fearful of the potential financial loss associated with online transactions, and 30% of consumers lost contact with the halal meat supplier (Reddy & Reddy, 2014).

Table 2: Financial Losses reported

Domain	**Impact ($)**
Indonesian cyber attack	7000
General sources reporting the 2007 financial losses reported	7.6 million
Bank Transfer fraud victimization as per 2019	3.4 billion

Cybercrime forum attacks financial losses reported in 2009	19.4 billion

The risk study highlighted dangers, and the magnitude of losses was evaluated as one of the most significant prospects of shopping online for sensitive shopping websites that govern and regulate the purchase and sale of halal meat in Malaysia. Security audits were deemed a practical solution based on seller interviews; however, according to various research papers, the audit yielded only 54% of results, and the companies that considered a security audit for their websites performed below the average level, with those at risk of cyber security and data loss included.

4.2 Findings from survey

The descriptive analysis determined the data's response orientation and normalcy. According to Table 3, the survey elicited responses from 200 individuals. The evidence is consistent across all three metrics. The skewness estimate for the halal logo and packaging is 0.116, the skewness estimate for authorities' enforcement and exposure is 0.301, and the skewness estimate for customer attitude is 0.43. These values are within the accepted range of -1+1, indicating standard data. Additionally, the mean scores suggest that respondents rated the questionnaire's assertions well. These findings show that respondents agreed with the questionnaire's statements.

Table 3: Descriptive results

	N	Minimum	Maximum	Mean	Std. Deviation	Skewness	
	Statistic	Statistic	Statistic	Statistic	Statistic	Statistic	Std. Error
HLP	200	1.00	5.00	3.5444	1.08250	-.116	.117
AEE	200	1.00	5.00	3.6377	1.05029	-.301	.117
CA	200	1.00	5.00	3.7401	1.21646	-.437	.117

Table 4: Association among constructs

Regression			Estimate	S.E.	P
HLP	→	CA	.216	.055	.000
AEE	→	CA	.301	.046	.000

The findings of the regression analysis are summarized in Table 4. The halal emblem and packaging affected customer sentiments. The results imply that customers' negative perceptions of online food fraud cause them to be more cautious about the packaging and ingredients. There is a correlation between people's consciousness and perception (Ruslan et al., 2018). Consumer awareness of halal food fraud has increased, and customers are beginning to pay attention to food ingredients, packaging, and trademarks. This awareness enables people to spot counterfeit or bogus products.

5. Discussion

The study's findings imply that consumer and meat producer awareness of the issues can result in the control of industry-wide criminality. The government's and authorities' roles and actions are critical and should be increased to contain the rise of

online fraud and fraud inside the halal food supply chain. Meat is one of the most highly rated products on the planet, making it a prime target for fraud, and similar incidents frequently occur in Malaysia (Ab Talib et al., 2015; Ariffin et al., 2021). According to Jaswir et al. (2017), adulterating food items to substitute high-end and expensive ingredients with low-quality and inexpensive ingredients is widespread. These activities are also widely done in Malaysia because they jeopardize the sanctity of the faith, even though they pose no threat to the health or lives of the people. The use of non-halal ingredients in food preparation is a serious concern for the Muslim community and must be addressed. The current study's findings corroborate Mohayidin and Kamarulzaman (2014)'s finding that consumers prefer halal-certified items.

Thus, to combat the growing problem of halal food fraud, both the industry and enforcement authorities must be aware of the issues, certified products, halal emblems, ingredients, and packaging materials, and be prepared to report any fraudulent acts in practice. Additionally, processing and packaging activities are critical components of the food supply chain and ensure that products maintain their halal status. Consumers' curiosity and concern about contamination, non-halal methods for preparing products, particularly meat, and forbidden ingredients during food processing are significant concerns that must be addressed (Fauzy et al., 2014; Mohayidin & Kamarulzaman, 2014). In a recent assessment, Ahmad and Zafar (2018) reported that Malaysian control is based on inspection, law enforcement, and laboratory testing. Additionally, the fundamental issues associated with sustaining a halal food system have been discussed: authority and coordination among the many halal agencies, establishing a high level of food fraud, and fake news about halal items. Thus, as demonstrated in this study, it is critical to provide complete descriptions of Malaysian food regulations to educate relevant stakeholders about food-related crimes and risks. Food-related crimes are rising in Malaysia, with negative consequences for company owners and the food industry. The growth in food crime has ramifications for developing and developed countries and serves as a reminder to the global food supply chain that an alarming number of cases are brought forward each year. The consequences for the worldwide food supply chain and consumers are severe and must be addressed and contained to prevent further spread.

6. Limitations, suggestions, and implications

This study aimed to design a mixed-methods study to assess fraud victimization and cybercrime in the Malaysian meat sector. The rise of meat cartels poses a danger to Malaysia's food business and is detrimental to the meat industry. The study interviewed consumers and business owners in the industry and performed a poll to determine the impact of fraud on the industry's operation and customer perceptions. The study, however, had certain drawbacks. The interview and survey samples were both small. The study excluded members of halal agencies from both the survey and the interviews to give a balanced perspective. As a result, future research should focus on addressing these constraints.

Each year, the demand for meat production increases, and as a result, the growing fraud in the meat business is a cause for alarm. Most food crimes involving meat products involve meat adulteration, mislabeling, and ingredient manipulation.

Additionally, the substitution of halal meat for non-halal alternatives such as pork, dog, and so forth is increasing, and thus the findings of this study have consequences for halal agencies, policy developers, and company owners. The study's findings underscore the importance of establishing stringent policies for controlling and inspecting food items at each stage of production, processing, and packaging. The government and halal authorities must concentrate their efforts on developing unified legislation and procedures that will aid in the management of this crime. Additionally, programmes aimed at increasing consumer and company owner awareness can assist in the direction of halal food fraud.

References

Ab Talib, M. S., Hamid, A. B. A., & Zulfakar, M. H. (2015). Halal supply chain critical success factors: a literature. *Journal of Islamic Marketing, 6*(1), 44-71. https://doi.org/10.1108/JIMA-07-2013-0049

Abd Kadir, M. H., Rasi, R. Z. R. M., Omar, S. S., & Manap, Z. I. A. (2016). Halal supply chain management streamlined practices: Issues and challenges. *IOP Conference Series: Materials Science and Engineering. 160*(1) (pp. 012070). IOP Publishing. https://doi.org/10.1088/1757-899X/160/1/012070

Ahmad, I., & Zafar, M. A. (2018). Impact of psychological contract fulfillment on organizational citizenship behavior: Mediating role of perceived organizational support. *International Journal of Contemporary Hospitality Management, 30*(2), 1001-1015. https://doi.org/10.1108/IJCHM-12-2016-0659

Ariffin, M. M., RIZA, N. S. M., Hamid, A., AWAE, F., & NASIR, B. M. (2021). Halal food crime in Malaysia: An analysis on illegal meat cartel issues. *Journal of Contemporary Issues in Business and Government, 27*(2), 1407-1412. https://doi.org/10.47750/CIBG.2021.27.02.152

Ariz, D. (2000). American guarantee & liability insurance co. v. Ingram Micro. *Inc, 104*, 99-185.

Burden, K., & Palmer, C. (2003). Internet crime: Cyber Crime—A new breed of criminal? *Computer Law & Security Review, 19*(3), 222-227. https://doi.org/10.1016/S0267-3649(03)00306-6

Coleman, K. G. (2011). Cyber intelligence: The huge economic impact of cyber crime. *Retrieved October, 5*, 2012. https://breakinggov.com/2011/09/19/cyber-intelligence-the-huge-economic-impact-of-cyber-crime/

Copes, H., Kerley, K. R., Mason, K. A., & Van Wyk, J. (2001). Reporting behavior of fraud victims and Black's theory of law: An empirical assessment. *Justice Quarterly, 18*(2), 343-363. https://doi.org/10.1080/07418820100094931

Doocy, J. H., Shichor, D., Sechrest, D. K., & Geis, G. (2001). Telemarketing fraud: Who are the tricksters and what makes them trick? *Security Journal, 14*(3), 7-26. https://doi.org/10.1057/palgrave.sj.8340087

FAN, M.-y., & NUNYUIE, O. (2019). Investigating the Effects of Cyber Fraud on Customer Trust for Online Shopping: The Ghanaian Setting. *European Journal of Business and Management, 11*(36), 86-96. https://doi.org/10.7176/EJBM/11-36-10

Fauzy, N. N., Husna, Z., & Sundram, V. (2014). Factors Behind Third-Party Logistics Providers Readiness Towards Halal Logistics. *Available at SSRN 2540573*, 1-12. https://dx.doi.org/10.2139/ssrn.2540573

Gordon, L. A., Loeb, M. P., & Sohail, T. (2003). A framework for using insurance for cyber-risk management. *Communications of the ACM, 46*(3), 81-85. https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.705.9851&rep=rep1&type=pdf

Hong, I. B., & Cho, H. (2011). The impact of consumer trust on attitudinal loyalty and purchase intentions in B2C e-marketplaces: Intermediary trust vs. seller trust. *International journal of information management, 31*(5), 469-479. https://doi.org/10.1016/j.ijinfomgt.2011.02.001

Jaswir, I., Mirghani, M. E. S., Salleh, H. M., Ramli, N., Octavianti, F., & Hendri, R. (2017). An Overview of the Current Analytical Methods for Halal Testing. *Contemporary Issues and Development in the Global Halal Industry* (pp. 291-300). Springer Singapore. https://doi.org/10.1007/978-981-10-1452-9_27

Jing, X., Yan, Z., & Pedrycz, W. (2018). Security data collection and data analytics in the Internet: A survey. *IEEE Communications Surveys & Tutorials, 21*(1), 586-618. https://doi.org/10.1109/COMST.2018.2863942

Johnson, K. D. (2004). *Financial crimes against the elderly*. US Department of Justice, Office of Community Oriented Policing Services. https://www.popcenter.org/sites/default/files/problems/PDFs/crimes_against_elderly.pdf

Kashif, M., Javed, M. K., & Pandey, D. (2020). A surge in cyber-crime during COVID-19. *Indonesian Journal of Social and Environmental Issues (IJSEI), 1*(2), 48-52. https://doi.org/10.47540/ijsei.v1i2.22

Lewallen, J. (2021). Emerging technologies and problem definition uncertainty: The case of cybersecurity. *Regulation & Governance, 15*(4), 1035-1052. https://doi.org/10.1111/rego.12341

Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports, 7*, 8176-8186. https://doi.org/10.1016/j.egyr.2021.08.126

Mohayidin, M. G., & Kamarulzaman, N. H. (2014). Consumers' preferences toward attributes of manufactured halal food products. *Journal of International Food & Agribusiness Marketing, 26*(2), 125-139. https://doi.org/10.1080/08974438.2012.755720

Montowska, M., & Pospiech, E. (2010). Authenticity determination of meat and meat products on the protein and DNA basis. *Food Reviews International, 27*(1), 84-100. https://doi.org/10.1080/87559129.2010.518297

NACSA. (2022). National Cyber Security Agency. https://www.nacsa.gov.my/

Nasution, M., Rossanty, Y., Achmad Daengs, G., Sahat, S., Rosmawati, R., Kurniasih, N., . . . Suhardi, S. (2018). Decision support rating system with Analytical Hierarchy Process method. *Int. J. Eng. Technol, 7*(2.3), 105-108. http://dx.doi.org/10.14419/ijet.v7i2.3.12629

Putri, E. O. (2018). Intention Toward Halal and Organic Food: Awareness for Natural Content, Religiosity, and Knowledge Context. *KnE Social Sciences*. https://doi.org/10.18502/kss.v3i10.3425

Rajasekharaiah, K., Dule, C. S., & Sudarshan, E. (2020). Cyber Security Challenges and its Emerging Trends on Latest Technologies. *IOP Conference Series: Materials Science and Engineering. 981*(2) (pp. 022062). IOP Publishing. https://doi.org/10.1088/1757-899X/981/2/022062

Reddy, G. N., & Reddy, G. (2014). A study of cyber security challenges and its emerging trends on latest technologies. *arXiv preprint arXiv:1402.1842*. https://doi.org/10.48550/arXiv.1402.1842

Rejeb, A. (2018). Halal meat supply chain traceability based on HACCP, blockchain and internet of things. *Acta Technica Jaurinensis, 11*(1). https://ssrn.com/abstract=3319432

Ruslan, A., Kamarulzaman, N., & Sanny, M. (2018). Muslim consumers' awareness and perception of Halal food fraud. *International Food Research Journal, 25*, S87-S96. http://mymedr.afpm.org.my/publications/85144

Saban, K. A., McGivern, E., & Saykiewicz, J. N. (2002). A critical look at the impact of cybercrime on consumer Internet behavior. *Journal of Marketing Theory and Practice, 10*(2), 29-37. https://doi.org/10.1080/10696679.2002.11501914

Sabillon, R., Cavaller, V., Cano, J., & Serra-Ruiz, J. (2016). Cybercriminals, cyberattacks and cybercrime. *2016 IEEE International Conference on Cybercrime and Computer Forensic (ICCCF)* (pp. 1-9). IEEE. https://doi.org/10.1109/ICCCF.2016.7740434

Said, H. (2017). Maqis seizes containers of unseparated halal, non-halal meat at Tanjung Pelepas. https://www.nst.com.my/news/crime-courts/2017/07/258158/maqis-seizes-containers-unseparated-halal-non-halal-meat-tanjung

Saini, H., Rao, Y. S., & Panda, T. C. (2012). Cyber-crimes and their impacts: A review. *International Journal of Engineering Research and Applications, 2*(2), 202-209. https://www.researchgate.net/profile/Hemraj-Saini/publication/241689554

Schoepfer, A., & Piquero, N. L. (2009). Studying the correlates of fraud victimization and reporting. *Journal of Criminal Justice, 37*(2), 209-215. https://doi.org/10.1016/j.jcrimjus.2009.02.003

Shichor, D., Sechrest, D. K., & Doocy, J. (2001). Victims of Investment Fraud. In N. P. Henry & S. David (Eds.), *Contemporary Issues in Crime and Criminal Justice: Essays in Honor of Gilbert Geis* (pp. 81-96). Prentice Hall Publishing. https://www.ncjrs.gov/App/abstractdb/AbstractDBDetails.aspx?id=193107

Siahaan, A. P. U. (2018). Pelanggaran cybercrime dan kekuatan yurisdiksi di Indonesia. *Jurnal Teknik dan Informatika, 5*(1), 6-9. https://journal.pancabudi.ac.id/index.php/Juti/article/download/82/66

Smith, A. D. (2004). Cybercriminal impacts on online business and consumer confidence. *Online Information Review, 28*(3), 224-234. https://doi.org/10.1108/14684520410543670

Spink, J., & Moyer, D. C. (2011). Defining the public health threat of food fraud. *Journal of food science, 76*(9), R157-R163. https://doi.org/10.1111/j.1750-3841.2011.02417.x

Tharshini, N., Hassan, Z., & Mas'ud, F. H. (2021). Cybercrime Threat Landscape amid the Movement Control Order in Malaysia. *International Journal of Business and Society, 22*(3), 1589-1601. https://doi.org/10.33736/ijbs.4323.2021

Yucedal, B. (2010). *Victimization in cyberspace: An application of Routine Activity and Lifestyle Exposure theories.* [Doctoral dissertation]. Kent State University. http://rave.ohiolink.edu/etdc/view?acc_num=kent1279290984

Zakaria, Z. (2008). Tapping into the world halal market: some discussions on Malaysian laws and standards. *Jurnal Syariah, 16*(3), 603-616. https://ejournal.um.edu.my/index.php/JS/article/view/22760

Zheng, M., Robbins, H., Chai, Z., Thapa, P., & Moore, T. (2018). Cybersecurity research datasets: taxonomy and empirical analysis. *11th USENIX Workshop on Cyber Security Experimentation and Test (CSET 18).* https://www.usenix.org/conference/cset18/presentation/zheng