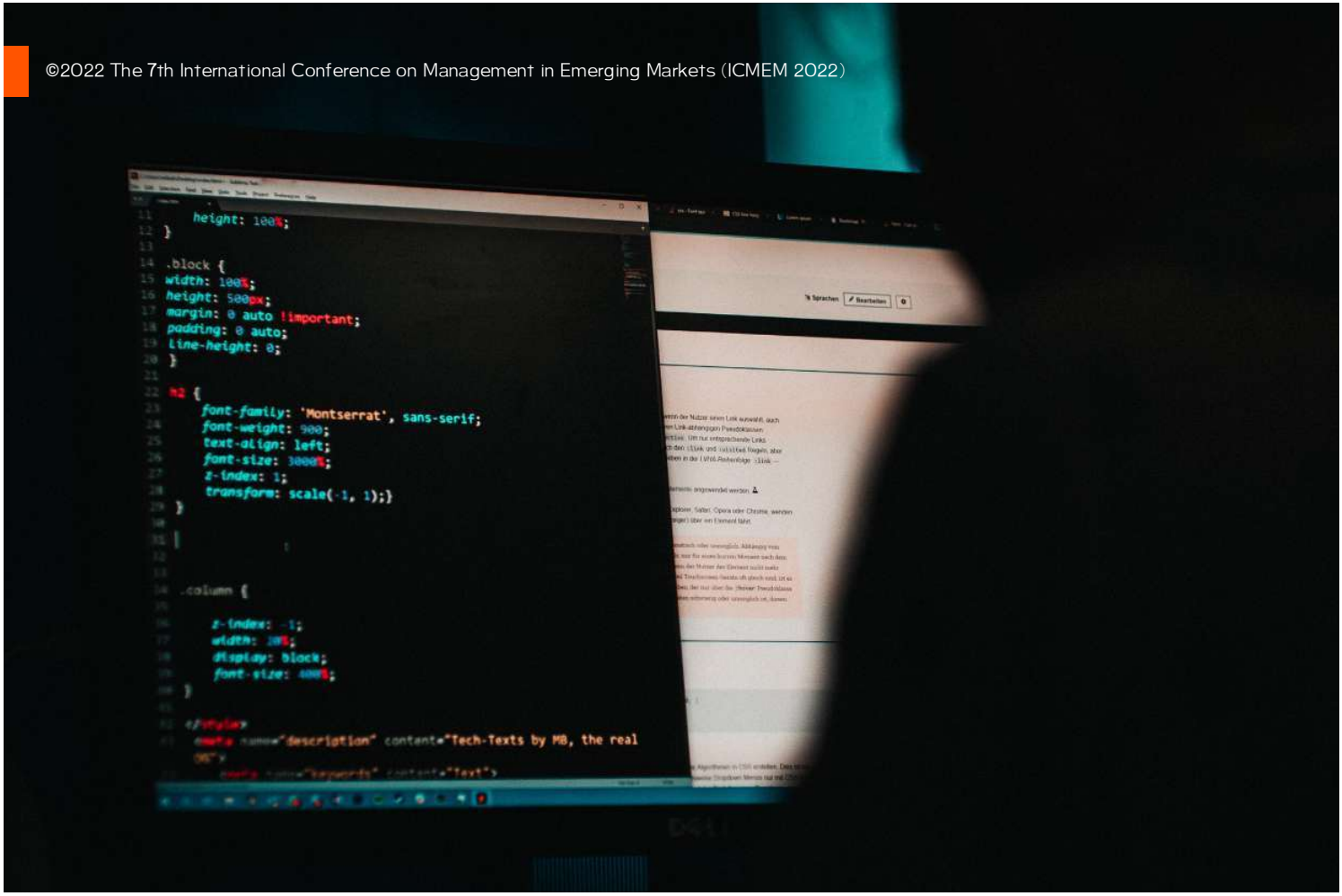

Paper 63

Customer's Cybersecurity Awareness in Indonesian Online Clothing Micro, Small and Medium Enterprises

Rio Paco Andiva

ICMEM

The 7th International Conference on Management in Emerging Markets

Abstract - **In the current technological era, almost every business operation and transaction are conducted through cyberspace, including micro, small and medium enterprises (MSME). However, MSMEs pose the greatest vulnerability to cyber-attacks due to their limitation in both awareness and resources. Multiple research found that people significantly affect cybersecurity more than the technical aspect. Thus, making cybersecurity awareness vital for every business, especially MSMEs. Currently, most cybersecurity awareness research is focused on the perspective of MSMEs and their owners. Limited cybersecurity awareness research assesses MSMEs in Indonesia, especially in the online clothing sector. This research will contribute to assessing cybersecurity awareness from MSME customers' perspective and aims to recommend Indonesian online clothing MSME environment to raise cybersecurity awareness. The researcher used a survey and a semi-structured interview to assess the overall cybersecurity awareness of Indonesian online clothing MSME customers. The semi-structured interview also explored respondents' opinions on raising cybersecurity awareness in the Indonesian online clothing MSME. The result shows a variety of levels of cybersecurity awareness among respondents. Correlation tests were conducted and found several aspects that were affecting respondents' cybersecurity awareness. The interview results also support the findings in the survey whilst also contributing to providing recommendations to raise cybersecurity awareness.**

Keywords – **Customers, Cybersecurity, Cybersecurity Awareness, Cyber-attack, MSME**

I. INTRODUCTION

Almost all businesses, including micro, small and medium enterprises (MSME) in Indonesia, are conducting business operations and transactions through cyberspace. Making up 99.99% [7] of businesses in Indonesia, MSMEs play a strategic role and are the most resilient sector in the country [16]

According to [20], Indonesia's internet penetration rate in 2017 was 51%, making it the third-largest Asia-Pacific region. MSMEs in Indonesia are seen utilising the opportunity and shifting their businesses online. Research by [15] projected that Indonesia's online economy will grow to $146 billion by 2025. However, cybersecurity threats will also be expected to grow significantly. Referring to research by Kaspersky in 2020, there were 192,000 recorded cyberattacks on Indonesian MSMEs [34]. Thus, making cybersecurity an essential factor for every business managerial consideration.

Contrary to popular belief, people significantly affect cybersecurity more than the technical aspects. Maria Vello in [23], a former CEO of Cyber Defence Alliance, says people are the weakest aspect of cybersecurity. Vello also argued that technology is not enough, and behavioural change is needed. Similarly, [29] found that people can be a weakness in cybersecurity, yet can be the first line of defence against cyberattacks with adequate training. However, MSMEs are vastly exposed to cyber-attacks due to their limited awareness and resources. [19] argued that the primary resource limitation is the organisation's budget, management, employee support and commitment toward cybersecurity. Additionally, MSME owners believe that their business is too small or not worth being attacked by criminals [29] This is where cybersecurity awareness implementation is needed.

Referring to (European commission) [2] argue that losing company data, especially customer data, is a significant concern for many businesses. According to [5] businesses could suffer financial loss, reputation damage, regulatory intervention, business disruptions and customer liability if cybersecurity is breached. Moreover, cybercriminals often steal millions of credit card and personal data from customers by exploiting a security flaw in any computer with an internet connection [25].

A. Research Contribution

Previous research shows that effective cybersecurity awareness comes from the user's perspective and decision-making process [21]. Based on the Information Processing Model study, threat detection happens involuntarily and without awareness [26]. Therefore, awareness needs to be triggered so people can move to the second stage of the Information Processing Model, where human's primary responses to threats are activated. Hence, Online Clothing MSME customers can focus on reacting to cybersecurity threats [4]. When customers understand how to react to cybersecurity threats, MSME owners will also react by ensuring that their business is cyber-safe to ensure they don't lose their customer's trust. Hence, raising cybersecurity awareness is essential

to improve the online MSME in Indonesia, especially in the clothing sector.

Currently, there is limited research in Indonesia that explicitly assesses cybersecurity awareness towards MSMEs, especially in the clothing sector. Understanding that cyberattacks on businesses, especially MSMEs, could also affect the customers, this research will assess the customers' perspectives. This research also aims to provide recommendations to raise cybersecurity awareness in the Indonesian online clothing MSME environment. Furthermore, this research could also be a foundation or guidance for further research to develop plans for improving the cybersecurity environment in Indonesian MSME.

B. Indonesian Online Clothing MSME

The researcher focused on assessing the Indonesian online clothing MSME based on observation of the researcher's environment, where many people started an online clothing business during the Covid19 pandemic. The researcher saw this as a business with a low entry barrier as most business processes are conducted online. Supporting this observation, a 2020 Indonesian National Bureau of Statistics research shows that clothing is the third largest MSME sector, accounting for 14.05%, just after food & beverages and wooden industries [6]. The same research also found that clothing MSME is the second largest internet user after the food & beverage sector in the whole MSME environment, with 22.66% [6].

C. Definitions

Based on Indonesian law number 28 of 2008, the criteria for micro, small and medium enterprises are explained in the table below

Table 1 - CRITERIA OF MSME IN INDONESIA

* Based on the exchange rate at 4th May 2022

Type	Minimum Asset (Rp)	Maximum Asset (Rp)	Annual Sales Revenue (Rp)	Annual Sales Revenue (£)*
Micro		50,000,000	< 300,000,000	< 16,500
Small	50,000,000	500,000,000	300,000,000 – 2,500,000,000	16,500 – 137,500
Medium	500,000,000	10,000,000,000	2,500,000,000 – 50,000,000,000	137,500 – 2,750,000

According to several resources [22][28][18], the definition of cybersecurity has emphasised an action to protect or defend from the risk of cyberattacks. At the same time, awareness is defined by [9][35][3] as an understanding or knowledge of a given situation. Hence, cybersecurity awareness means activities that focus individuals' attention on cybersecurity issues, allowing individuals to recognise cybersecurity concerns and respond accordingly.

D. Types of Cyberattack

A cyberattack is an attack via cyberspace, targeting enterprises' use of cyberspace to disrupt, disable, destroy, or maliciously control a computing environment/ infrastructure, destroy the integrity of the data, and steal controlled information [22]. Combining research from [10][12][13], eight types of cyberattacks mainly occur to MSMEs: Hacking, Virus, Ransomware, Spyware, Denial of Service (DoS), Phishing, Identity theft and DNS Tunnelling. The table below will explain the definition of each type of cyberattack.

Table 2 - DEFINITIONS OF CYBERATTACKS

Types of Cyberattack	Definition
Hacking	Hacking is an activity that compromises the confidentiality or integrity of a system. It requires a certain skill and involves exploiting the system's vulnerability to break into the system [24].
Identity Theft	Identity Theft is when the attacker pretends to be a different person to gain financial benefits [31].
Phishing	Phishing attempts to convince the victim to act on the pretence of engaging with a legitimate party [24].
Virus	A virus is a computer program that can copy and infect a computer without the user's permission or knowledge. A virus can then corrupt or delete data on a computer, use email to spread itself to other computers, or even erase everything on a hard disk [22].
Spyware	Spyware is still considered Malware, specifically designed for information gathering from its victim [22].
Ransomware	Ransomware. An extortive Malware locks a user's data to get payment for unlocking the data [31].
Denial of Service (DoS)	Denial of service (DoS) or Distributed Denial of Service (DDoS) is an attack that floods systems, servers, and networks with traffic to exhaust resources and bandwidth. This eventually results in the system being unable to process legitimate requests [32].

Types of Cyberattack	Definition
DNS Tunnelling	DNS tunnelling works by packaging data into DNS packets to be sent in a query for a specific domain [37]. It is exploited by embedding illegal data packed as a legitimate DNS packet. DNS traffic can travel across the network without interference because the hosts often trust the information of DNS queries [36]

E. Human Factors in Cyberattacks

After understanding the various types of cyberattacks, the human factor is a crucial part that attackers often exploit. For instance, viruses that need an execution order from the victim before causing damage [31] and when Malware enters the victim's system by clicking a malicious link from email attachments or installing risky software [32] Vello further argued with [23] that no technology could stop social engineering or human nature. [17] further explains that attackers increasingly target humans as they are often seen as the weakest link in the system.

F. Measures to Protect from Cyberattacks

This research will use the combination of various cybersecurity measures provided by The U.K. National Cyber Security Centre (NCSC) and The Indonesian Ministry of Communication and Information. The suggested cybersecurity measures can be seen in the list below:

1. Avoid using public Wi-Fi as much as possible, especially when accessing sensitive information [27]
2. Use antivirus, turn on the firewall and regularly patch & updating the software to avoid malware damage [27]
3. Don't open a link or attachment from unknown sources [27]
4. Periodically changing passwords, using special characters & irregular sentences and using a password manager [27]
5. Shop only from trusted brands with positive reviews and security icons [13]
6. Avoid sharing personal information by using a fake name or a fake email address [13]

G. Related Literature

Several related works of literature have been conducted to assess cybersecurity awareness [30] listed 24 articles in his paper "Systematic Literature Review of Approaches to Assessing Cybersecurity Awareness". The researcher chose five research that is related and applicable to this research shown in the table below

Table 3 - RELATED LITERATURE

Based on (Rahim et al.)

Author(s)	Objective	Scope of Assessment
Furnell et al. (2007)	To identify internet users' awareness of cyber threats and their understanding of the methods for protecting and safeguarding data and systems over the internet	Level of cybersecurity awareness
Rezgui and Marks (2008)	To explore the level of information security awareness	Cybersecurity in general and the level of cybersecurity awareness
Furnell et al. (2008)	To provide a rich source of users' experiences and views regarding internet security and issues of online protection	Cybersecurity in general
Furman et al. (2012)	To identify the correct perception, myths and potential misperceptions about computer security	Cybersecurity in general

II. METHODOLOGY

A. Research Design

This research used a mixed-method of survey and semi-structured interview. The survey enabled the researcher to assess the cybersecurity awareness of a large customer population. In contrast, the semi-structured interview provided a deeper understanding of the respondent's view on cybersecurity awareness, which eventually generated recommendations to raise cybersecurity awareness for the online clothing MSME customers in Indonesia.

B. Data Collection

The survey consisted of 20 questions, first asking the respondent's agreement with the research ethics disclaimer. The other 19 questions are demographic questions, online shopping frequency & cybersecurity familiarity, familiarity with eight types of cyberattacks, and cybersecurity implementation.

The semi-structured interviews were conducted through Google meets and WhatsApp video calls. The interview audio was recorded with prior agreement from the

respondent. The respondents were presented with 21 questions that were divided into six different sections according to the question's objectives. In addition, probing questions were asked during the interview to clarify the respondent's answers or to explore new ideas generated by the respondents.

C. Sampling Technique

The survey sample was any Indonesian aged 17 and over who had experience purchasing a clothing item from online MSMEs. According to the survey in 2020 conducted by the Indonesian National Bureau of Statistics, the percentage of the Indonesian population with access to the internet is 53.73% [7] Meanwhile, the latest census in 2020 recorded that the total population in Indonesia was 270,203,917 people [8]. Therefore, the population frame to obtain the sample is 145,180,565 people. The survey used a simple random sampling technique that gives every individual an equal chance of being selected in a population sample [1]. Using Yamane's formula, the targeted survey sample was 156 respondents.

The interview respondent's requirement was the same as the survey. According to [11] considering the time constraint and the limitations, the interview was conducted with five respondents.

D. Analysis

The survey was analysed by SPSS software. Descriptive statistics were used to explain the general findings of the research combined with Spearman Rank Correlation to test the statistical significance between variables.

The interview was analysed based on the thematic analysis method that focuses on finding themes or patterns observed in the interview [33]. The transcribed interviews were then coded using NVivo software and explained in detail using a matrix.

E. Validity and Reliability

The survey validity test was conducted using Pearson Product-Moment Correlation. The total respondent was 261, and the r-value from the table with 5% significance is 0.121. The correlation coefficient was tested using SPSS to 10 Likert-scale questions, as seen in the table below:

Table 4 - PEARSON CORRELATION VALIDITY

**Correlation is significant at the 0.01 level (2-tailed)

Questions	Pearson Correlation	R-Value	Validity
Cybersecurity Term	0.751**	0.121	Valid
Hacking	0.777**	0.121	Valid
Identity Theft	0.792**	0.121	Valid
Phishing	0.821**	0.121	Valid
Virus	0.689**	0.121	Valid
Spyware	0.829**	0.121	Valid
Ransomware	0.819**	0.121	Valid
Denial of Service (DoS)	0.751**	0.121	Valid
DNS Tunnelling	0.702**	0.121	Valid
Cyberattack Victim Likeliness	0.298**	0.121	Valid

For all questions, the Pearson correlation coefficient was larger than the r-value. Therefore, all of the questions were valid.

The survey Reliability was tested using Cronbach's Alpha in SPSS, as shown in the table below:

Table 5 - CRONBACH'S RELIABILITY

Total Questions	Cronbach's Alpha	Reliability
10	0.904	Reliable

The Cronbach's Alpha result shows it is bigger than the most commonly accepted Cronbach's Alpha of 0.600 [14]. Therefore, the survey questions were reliable.

The interview method in this research was semi-structured to ensure every respondent was faced with the same questions. Respondents were chosen by their experience purchasing online clothing items from Indonesian MSMEs. In addition, the researcher tried to diversify the respondent by recruiting respondents with different education levels and occupations. The interview tone was also conducted professionally to ensure neutrality and reduce bias. As the objective of this research, the findings were applicable to generate recommendations to raise cybersecurity awareness in the Indonesian online clothing MSME environment.

F. Ethical Consideration

This dissertation project was conducted according to the University of Hull's ethical principles. The researcher signed an ethics form that the Supervisor approved. During the data collection, research participants were also informed about their voluntary rights to withdraw from the research at any time, and their personal information will not be revealed in any way.

G. Limitations

Because this research is assessing a specific sector of MSME in Indonesia and there were very limited resources available, this research mostly relied on academic resources in another country. Therefore, some of the most applicable resources were researched that targeted the Asia-Pacific region.

The research was entirely conducted in English, with the respondents requiring the research to be completed in Indonesian. As a result, several terms gained from English resources must be translated to Indonesian with the researcher's limited ability. In addition, some terms related to cybersecurity awareness have not yet had an equivalent translation in Indonesian.

Reaching a large number of survey respondents is also another challenge. The survey result was biased because the sample demographic proportion did not represent the actual demographic of Indonesia.

There is also an ethical limitation where the researcher cannot collect the respondent's contact. Collecting the respondent's contact would have been beneficial in inviting the respondent for an interview to explore the topic further.

III. RESULTS

A. Survey

Two hundred sixty-one respondents were obtained using the Google Form platform. The survey used multiple choices and a 4-point Likert scale that was analysed using descriptive statistics and Spearman Rank Correlation Coefficient using SPSS.

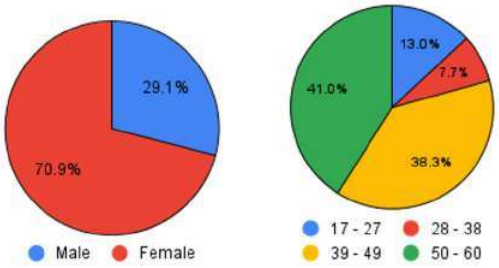

Fig. 1 Survey Gender and Age Range Pie Chart

Females dominated the survey respondents by 71%, with a total of 185 respondents. On the other hand, male respondents were 29%, with a total of 76 respondents. Meanwhile, respondents with the age range of 50-60 and 39-49 shared the biggest proportion, with a total of 107 (41%) and 100 (38%) respondents, respectively. This was followed by the age range of 17-27 with 34 (13%) respondents and 28-38 with 20 (8%) respondents.

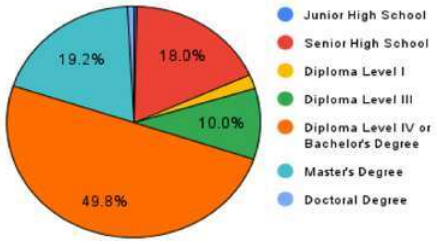

Fig. 2 Education Level

The respondents dominated the survey with higher education levels, with 130 (49,8%) completing Diploma Level IV or a Bachelor's degree and 50 (19.2%) completing a Master's degree. In addition, two respondents have a doctoral degree. Meanwhile, 26 (10%) respondents had a Diploma level III. Furthermore, 47 (18%) respondents completed Senior High School level.

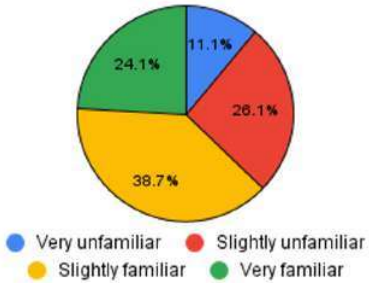

Fig. 3 Familiarity With "Cybersecurity" Term

The survey asked how familiar the respondents were with the term "cybersecurity", and 101 (38.7%) of respondents were slightly familiar with the term. There was a similar proportion of respondents who felt very familiar with the respondents who felt slightly unfamiliar, with 63 (24.14%) and 68 (26.05%), respectively. On the other hand, 29 (11.11%) respondents felt very unfamiliar with the term.

The respondents were also asked how familiar are they with eight types of cyberattacks using a 4-level Likert scale, and the result is shown in the table below:

Table 6 - TYPES OF CYBERATTACK FAMILIARITY

Types of Cyberattack	Average Answer	Familiarity
Hacking	2.88	Slightly familiar
Identity Theft	2.78	Slightly familiar
Phishing	2.37	Slightly unfamiliar
Virus	3.1	Slightly familiar
Spyware	2.38	Slightly unfamiliar
Ransomware	1.99	Slightly unfamiliar
Denial of Service (DoS)	1.95	Slightly unfamiliar
DNS Tunnelling	1.7	Slightly unfamiliar

As seen in the table above, most respondents were slightly familiar with Hacking, Identity theft, and Virus. At the same time, the respondents are slightly unfamiliar with the other five types of cyberattacks. The virus had the highest familiarity among the respondent, while DNS Tunnelling had the lowest.

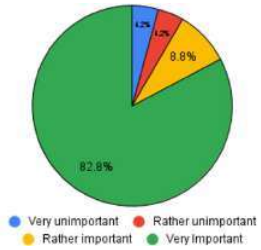

Fig. 4 The Importance of Keeping Personal Information Safe

Almost all respondents believe keeping their personal information safe while conducting an online transaction is essential. However, 23 (8.81%) respondents felt it was just rather important. Furthermore, there was an equal number of 11 (4.2%) respondents who believed that it was rather unimportant and very unimportant.

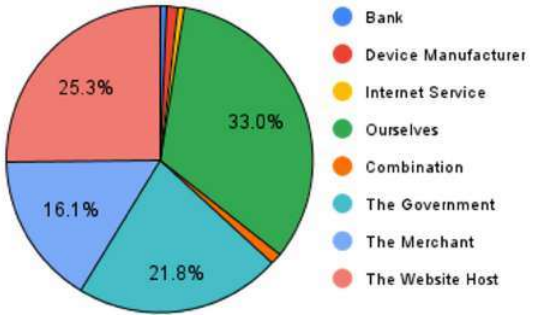

Fig. 5 Cybersecurity Responsibility

According to the respondents, the four largest parties responsible for cybersecurity are ourselves (33%), the website host (25.3%), the government (21.8%) and the merchant (16.1%). The realisation that cybersecurity is our own responsibility had the highest response of 86 respondents.

A correlation test was conducted using Spearman Rank Correlation Coefficient to five variables to analyse the survey findings.

Table 7 - CYBERSECURITY TERM FAMILIARITY CORRELATION

** Correlation is significant at the 0.01 level (2-tailed)

"Cybersecurity Term Familiarity"			
	Correlation Coefficient	Sig. (2-tailed)	N
Types of Cyberattack	.668**	0.000	261
Cybersecurity Importance	.181**	0.003	261
Cyberattack Experience	.169**	0.006	261
Cybersecurity Measures	0.003	0.964	261

The table shows a correlation between respondents' familiarity with the term "cybersecurity" with the types of cyberattack, cybersecurity importance and cyberattack experience. However, there is no correlation with cybersecurity measures taken by the respondents.

Table 8 - EDUCATION LEVEL CORRELATION

** Correlation is significant at the 0.01 level (2-tailed)

"Education Level"			
	Correlation Coefficient	Sig. (2-tailed)	N
"Cybersecurity" Familiarity	0.082	0.185	261
Types of Cyberattack	.161**	0.009	261
Cybersecurity Importance	0.007	0.913	261
Cybersecurity Responsible	0.069	0.266	261
Cyberattack Experience	0.071	0.250	261
Cybersecurity Measures	0.051	0.408	261

The table shows a correlation between respondents' familiarity with the term "cybersecurity" with the types of cyberattack, cybersecurity importance and cyberattack experience. However, there is no correlation with cybersecurity measures taken by the respondents.

Table 9 - PURCHASING FREQUENCY CORRELATION

** Correlation is significant at the 0.01 level (2-tailed)

"Purchasing Frequency"			
	Correlation Coefficient	Sig. (2-tailed)	N
"Cybersecurity" Familiarity	.136*	0.028	261
Types of Cyberattack	.142*	0.021	261
Cybersecurity Importance	0.093	0.136	261
Cybersecurity Responsible	0.080	0.198	261
Cyberattack Experience	0.090	0.147	261
Cybersecurity Measures	0.052	0.403	261

The table shows that respondents' purchasing frequency only correlated to familiarity with the term "cybersecurity" and different types of cyberattacks. There was no correlation with the other four cybersecurity aspects.

Table 10 - LIKELINESS CORRELATION

"Likeliness to be a Cyberattack Victim"			
	Correlation Coefficient	Sig. (2-tailed)	N
Cyberattack Experience	0.056	0.368	261
Cybersecurity Measures	-0.009	0.888	261

The result shows no correlation between the respondent's likeliness of being a cyberattack victim with cyberattack experience and cybersecurity measures they have taken.

Table 11 - CYBERSECURITY IMPORTANCE CORRELATION

"Cybersecurity Importance"			
	Correlation Coefficient	Sig. (2-tailed)	N
Cybersecurity Responsibility	-0.016	0.794	261
Cyberattack Experience	0.037	0.556	261
Cybersecurity Measures	-0.019	0.763	261

The table shows no correlation between respondents' understanding of cybersecurity importance with cybersecurity responsibility, cyberattack experience, and cybersecurity measures.

B. Interview

The semi-structured interview was conducted with five respondents with various occupations (see table 12 below) using the Google Meets platform. The transcribed interview result was then analysed using NVivo software. The analysis will discuss the respondent's cybersecurity awareness, cybersecurity measures taken by the respondents and respondent's opinions on raising cybersecurity awareness in the Indonesian online clothing MSME environment.

Table 12 - INTERVIEW RESPONDENT PROFILE

Respondent's Name	Completed Education Level	Occupation
Respondent A	Senior High School	Student
Respondent B	Bachelor's Degree	Diver
Respondent C	Bachelor's Degree	UI/UX Designer
Respondent D	Senior High School	F&B Entrepreneur
Respondent E	Diploma Level III	Occupational Therapist

All respondents were asked how familiar they are with the term "cybersecurity" and to elaborate on their understanding of it. The most mentioned word from the respondents was data, purchase and risk. The respondent's response is shown in the table below:

Table 13 - CYBERSECURITY AWARENESS ELABORATION

	Responses		
	Data	Purchase	Risk
Res. A		"… whether it's about purchase…"	"… digital world, the risk will be higher.."
Res. B	"… it's about keeping our data safe"		
Res. C	"… how we protect our data…"		"… avoid the risk of breach…"
Res. D	"… submitting personal data…"	"… when conducting an online transaction…"	
Res. E	"I think it's personal data security…"	"… when we shop online"	"… I understand several risks…"

Most respondents defined cybersecurity as protecting personal data while conducting an online transaction or purchase. However, as [22] argues, cybersecurity is about protecting and defending against cyberattack risks. Two respondents included risk as part of their understanding. Along with the themes mentioned above, two respondents defined cybersecurity in the context of cyberspace and social media.

Respondents were also asked how familiar they were with eight types of cyberattacks. Their response is shown in the table below:

Table 14 - CYBERATTACK FAMILIARITY

	Responses				
	Res. A	Res. B	Res. C	Res. D	Res. E
Hacking	Familiar	Familiar	Familiar	Familiar	Familiar
Identity Theft	Familiar	Familiar	Familiar	Familiar	Familiar
Virus	Familiar	Familiar	Familiar	Familiar	Familiar
Phishing	Familiar	Familiar	Familiar	Familiar	Unfamiliar
Spyware	Familiar	Familiar	Familiar	Unfamiliar	Unfamiliar
Ransomware	Familiar	Familiar	Familiar	Unfamiliar	Unfamiliar
Denial of Service	Unfamiliar	Familiar	Familiar	Unfamiliar	Unfamiliar
DNS Tunnelling	Unfamiliar	Unfamiliar	Familiar	Unfamiliar	Unfamiliar

All interview respondents were familiar with Hacking, Identity Theft and Virus. On the other hand, DNS Tunnelling is the most unfamiliar type of cyberattack, according to the respondents.

Respondents were asked how they ensure their cybersecurity when purchasing an online clothing item from MSME in Indonesia. The most recurring theme was respondents using a third party to increase their security. There were also other measures taken by the respondents shown in the table below:

Table 15 - ENSURING CYBERSECURITY

	Res. A	Res. B	Res. C	Res. D	Res. E
3rd Party Security		"… third party will take part in the transaction …"		"… third party such as e-commerce …"	"… used e-commerce platform as a third party"
Be Generally Careful				"… very careful uploading my phone number and address …"	"… avoid using full name, only first name …"
Only Trusted Brands		"… I look for brands that guarantees the security …"	"… purchase from trusted websites …"		
Reviews		"… positively reviewed by the public …"	"… feedback and reviews from the other customers …"		

Three respondents saw the third party as an additional layer of security that can be trusted. For example, respondent B refers to the third party as the payment gateway, while respondents D and E use e-commerce platforms as the transaction intermediary. Furthermore, respondents D and E also being cautious regarding their names, phone numbers and home address. Another theme is brand trust, where respondents choose the brand based on their reviews and feedback from other customers.

The interview also explored what kind of features or signs that in their opinion, makes MSME brands or websites safe for the transaction. Their responses will be shown in the table below:

Table 16 - CONSIDERATION OF CHOOSING MERCHANTS

	Responses				
	Res. A	Res. B	Res. C	Res. D	Res. E
Online store display		"… indication that the website is active with many customers …"	"… presentable website"	"… website that are developed, active, and maintained"	"… great display of the website …"
Review or testimony	"… look for testimony of review from previous customers …"	"… I would be looking at the review …"			"… the number of reviews …"
Reputation	"… data leak, bad reputation or other news …"			"… I choose the brand with the highest reputation …"	
Multiple contacts	"I trust merchants that provides contacts and have an offline store"				"… many different forms of communication …"

The interview result shows that visually pleasing MSME's online store is one sign that makes respondents trust them. Respondents then look into the merchant's review or testimony and seek the merchant's reputation. Furthermore, providing multiple forms of communication shows the merchant can be reached by the customers and are safe.

The interview asked respondents where their primary source of learning about cybersecurity is. The researcher also asked the respondents what they thought was the most interesting and the easiest way to learn about cybersecurity. Finally, the respondents were offered to recommend how to raise cybersecurity awareness in the Indonesian online clothing environment. The respondent's response can be seen in the three tables below:

Table 17 - SOURCE OF LEARNING

	Responses				
	Res. A	Res. B	Res. C	Res. D	Res. E
Academics	"… I'm currently taking a cybersecurity course in University …"	"… I studied about it in University …"	"… one of my course in my computer science degree …"		
Self-Taught	"… try to protect myself and learn some…"				"I have read several articles …"
Friends and family	"… talked about it with my fellow gaming friends …"			"I have a friend that specialise in this aspect …"	

The respondents had a variety of sources of learning. Most respondents learned about cybersecurity in a formal higher education such as University. Some others also taught themselves and read articles. There were also friends and family involved in learning about cybersecurity

Table 18 - LEARNING ABOUT CYBERSECURITY

	Responses				
	Res. A	Res. B	Res. C	Res. D	Res. E
Academics	"… we can also learn from scholarresearches …"		"… you can take courses in any educational institutions …"		"… articles would be a great source to learn about cybersecurity …"
Social Media		"… many educational account in social media that talks about cybersecurity …"	"… plenty of sources are available in Google or YouTube …"		"… though social media such as TikTok and Instagram …"
Friends and family	"… ask a friend or family about cybersecurity …"				"… smallest environment, which is family …"

Respondents believed that the best way to learn about cybersecurity is through the academic environment and social media. On the other hand, some respondents still believed that learning from friends or families is one of the best ways to learn about cybersecurity..

Table 19 - RESPONDENT'S RECOMMENDATION

	Responses				
	Res. A	Res. B	Res. C	Res. D	Res. E
Education Sector	"… introduce cybersecurity in formal education such as schools …"				"… should be included in school curriculum …"
Merchant Participation	"… merchants can be a part of it …"		"… business owners should invest in hiring experts …"		
Government Training					"… the government provide training programmes for MSME owners"

Furthermore, respondents were also asked how we can make cybersecurity learning interesting. However, there is no general theme that appeared. In contrast, every respondent provided different ways, such as movies and videos, Instagram filters, songs and slogans, games, community participation, joining a hackathon competition, and even waiting until they experienced a cyberattack themselves.

IV. DISCUSSION

This research aimed to assess Indonesian online clothing MSME customers' cybersecurity awareness and provide recommendations on raising cybersecurity awareness in the Indonesian online clothing MSME environment. The survey showed a different level of awareness for each aspect of cybersecurity. The interview further explored the respondent's understanding of cybersecurity and provided recommendations to raise cybersecurity awareness.

A. Customer's Cybersecurity Awareness

The survey result shows that 24.14% of the respondents were very familiar with the term "cybersecurity". Most respondents felt slightly familiar with the term sharing, 38.7% of the total respondents. The correlation test (see table 7) shows that the respondent's awareness is not limited to cybersecurity as a term, but also respondents are aware of the given types of cyberattack. The correlation also shows the more people familiar with the term "cybersecurity", the more important it is for the respondents to keep their personal information while conducting an online transaction. Moreover, the correlation also indicates the significance between the term familiarity and cyberattack experience. This might imply that experiencing a cyberattack contributes to respondents' cybersecurity awareness. The interview (see table 13) reveals that respondents can associate cybersecurity with risk, which is one aspect of cybersecurity in line with the literature review. Other than risk, respondents also associate cybersecurity with personal data and online transactions.

The following correlation test (see table 8) was between respondents' education level and other cybersecurity aspects. However, the test only shows the correlation significance between education level and types of cyberattacks. This implies that the higher the education level of the respondents, the more familiarity they have with different types of cyberattacks. The interview (see table 17) confirms this by showing three respondents' sources of learning about cybersecurity through formal educational institutions such as universities. This correlation test shows education level is a significant factor in customers' cybersecurity awareness.

Another correlation test (see table 9) was between purchasing frequency and other cybersecurity aspects. The higher the respondent's purchasing frequency, the higher their familiarity with different types of cyberattacks. The two significant correlations show that customers are aware of cybersecurity when purchasing a clothing items from online MSMEs in Indonesia. Customers are not only aware of cybersecurity as a term but also of the different types of cyberattacks. The interview (see tables 15 and 16) shows that respondents took several measures when selecting merchants. Three out of five respondents prefer a third party as an intermediary to ensure their transaction safety. Respondents were also careful about revealing their private information, limiting their transactions to trusted brands and checking the merchant's review. When selecting the merchant, the merchant's online store contributes significantly towards the respondent's trust along with the review or testimony, merchant's reputation and merchants that provide multiple forms of communication with the customers.

The correlation test of likeliness of being a cyberattack victim with cyberattack experience and cybersecurity measures shows no significant correlation. Customers' judgement on how likely they are to be cyberattacked has nothing to do with their cyberattack experience and the cybersecurity measures they have taken. The correlation test of customers' understanding of cybersecurity importance also shows no significance with cybersecurity responsibility, cyberattack experience and cybersecurity measures.

B. Recommendation to Raise Cybersecurity Awareness

This research shows the variety level of awareness among Indonesian online clothing MSME customers. The correlation test shows that education cybersecurity awareness correlates significantly to educational level. In general, making education accessible will also improve overall cybersecurity awareness in the Indonesian MSME environment. The interview respondent also recommends including a cybersecurity awareness program in the school curriculum.

Respondent A	"Maybe put some "spices" in formal education such as schools."
Respondent B	"think cybersecurity awareness should be included in the school curriculum as well."

Many respondents still believe that cybersecurity is another party's responsibility, such as the government, the website host and the merchant. However, people still do not realise that the most responsible party in cybersecurity is ourselves. While people expect the government, the website host and the merchant to be responsible for people's cybersecurity, it also provides an opportunity to address the misunderstandings among the people. As mentioned earlier, the government can include a cybersecurity awareness program in schools, starting a highly engaging campaign and providing training to those already involved in the MSME environment.

MSME owners can also participate by promoting their business through a secured website. The interview results

show that displaying a merchant's online store contributes to customer trust. Having a secured website might be a significant investment at first but will improve the MSME environment overall.

As individuals, we can raise our cybersecurity awareness by following educational accounts on social media, participating in a community, or reading trusted academic articles.

V. CONCLUSION AND RECOMMENDATION

A. Conclusion

This research aimed to assess the cybersecurity awareness of Indonesian online clothing MSME customers and to provide recommendations on raising cybersecurity awareness in the Indonesian online clothing MSME environment.

Based on this research's quantitative method of survey and qualitative method of interviews, we can conclude that most online clothing MSME customers in Indonesia are aware of cybersecurity and cyberattack risks. It is then supported by the strong correlation between the cybersecurity familiarity with types of cyberattack, customers' understanding of cybersecurity importance and cyberattack experience, which shows that customers understand beyond the term.

Education was an important factor that contributed to customers' cybersecurity awareness. A correlation was found between survey respondents' education level with the familiarity with several types of cyberattacks. The correlation is further supported by the interview where three respondents gain cybersecurity awareness through the academic environment. Interview respondents also believe that the academic environment is the best source of learning about cybersecurity.

Customer's awareness is also shown by the correlation between customers' shopping frequency, familiarity with cybersecurity terms and types of cyberattacks. The correlation indicates that customers are aware of the increasing cybersecurity risk parallel to the online shopping frequency. This correlation is also further supported by various cybersecurity implementations by interview respondents. Interview respondents' methods of minimising cybersecurity risks are mostly using 3rd party as a transaction intermediary, choosing reputable brands and relying on the brand's review or testimony.

Referring to the importance of this research, cybersecurity awareness from a customer's perspective was assessed. Hopefully, this research can raise cybersecurity awareness that is mostly overlooked in Indonesia, especially in Micro, Small and Medium enterprises environments. This research could be the foundation of Indonesian MSME customers' cybersecurity awareness and provide insights for further research in different MSME sectors.

B. Recommendation

Based on this research, there are various opportunities for all parties to be involved to raise cybersecurity awareness. All parties should take part in educating people that cybersecurity is our own responsibility.

The government could take part by focusing on policies in the education sector such as adding cybersecurity courses at multiple education levels. The government cyber and crypto agency could also start a cybersecurity educational campaign through various social media to reach people across different levels. Another method to be considered is adding cybersecurity to training that is provided to MSMEs.

For the MSME owners, building a customer's trust is beneficial for the business, and one of the methods is by having a well-displayed and secured website. It might be an expensive investment, in the beginning, to implement security features on the website, but will pay off in the future. When customer trust is built, MSME can promote and educate cybersecurity its customers.

Future research could address different sectors of Indonesian MSME to address the awareness level of both the merchant and the customers. It will also be beneficial for further studies to explore cybersecurity awareness in Indonesian online shoppers to provide better insights for the policymakers. Further research is needed to determine how effective each method of raising cybersecurity awareness in this research for a government policy to be implemented.

ACKNOWLEDGMENT

I would like to thank my Supervisor, Dr Antonio Malfense Fierro, for his help, guidance, feedback and support throughout my final year at the University of Hull. I would also like to thank Dr Dionysios Demetis, who motivated me to write a dissertation about cybersecurity and helped me along the way.

I must also thank my friends Agha, Audie, Lintang, Nizzah and Sazqi for their positive friendship throughout my three years at University, my family and my girlfriend Ailsya back home in Indonesia for always being there for me.

Finally, I would like to thank all survey and interview participants willing to contribute to my dissertation.

REFERENCES

1. Acharya, A., Prakash, A., Saxena, P. and Nigam, A., 2013. Sampling: why and how of it?.

2. Ameen, N., Tarhini, A., Shah, M., Madichie, N., Paul, J. and Choudrie, J., 2021. Keeping customers' data secure: A cross-cultural study of cybersecurity compliance among the Gen-Mobile workforce. Computers in Human Behavior, 114, p.106531.

3. APA Dictionary, n.d. Awareness. In: APA Dictionary of Psychology. [online] Washington DC: American Psychology Association. Available at: https://dictionary.apa.org/awareness [Accessed 3 May 2022].

4. Beck, A. and Clark, D., 1997. An information processing model of anxiety: Automatic and strategic processes. Behaviour Research and Therapy, [online] 35(1), pp.49-58. Available at: <https://reader.elsevier.com/reader/sd/pii/S0005796796000691?token=3B95BCFCC0DBC7133DFCBAD5FDE5BAE58AA8412B339E58A0D805332A746846E09EBC1AA8577E21F4BF4BC38E63E21676&originRegion=eu-west-1&originCreation=20211118112910>.

5. Berkman, H., Jona, J., Lee, G. and Soderstrom, N., 2018. Cybersecurity awareness and market valuations. Journal of Accounting and Public Policy, 37(6), pp.508-526.

6. BPS, 2020. MSME Industry Profile. Jakarta: Indonesian Bureau of Statistics, p.11.

7. BPS, 2020. Telecommunication Statistics in Indonesia. Jakarta: BPS Statistics Indonesia, p.19.

8. BPS, 2020. 2020 Census Result. Jakarta: BPS Indonesian Statistics, p.9.

9. Cambridge Dictionary, n.d. Awareness. In: Cambridge Advanced Learner's Dictionary & Thesaurus. [online] Cambridge: Cambridge University Press. Available at: <https://dictionary.cambridge.org/dictionary/english/awareness> [Accessed 3 May 2022].

10. CISCO, 2021. Cybersecurity for SMBs: Asia Pacific Businesses Prepare for Digital Defense. [online] Cisco Secure, p.10. Available at: <https://www.cisco.com/c/dam/global/en_sg/products/security/assets/data/cybersecurity-for-smbs-asia-pacific-businesses-prepare-for-digital-defense.pdf> [Accessed 2 May 2022].

11. Creswell, J.W. and Poth, C.N., 2016. Qualitative inquiry and research design: Choosing among five approaches. Sage publications.

12. DCMS, 2021. Cyber Security Breaches Survey 2021. London: Department for Digital, Culture, Media and Sport.

13. Donny, B. and Banyumurti, I., 2018. Keamanan Siber Untuk E-Commerce. Jakarta: Ministry of Communication and Information, p.46.

14. Ghozali, I., 2005. Aplikasi analisis multivariate dengan program IBM SPSS 25. Semarang: Universitas Diponegoro.

15. Google, Temasek & Company, B. (2021) Roaring 20s: The SEA Digital Decade Indonesia: Available online: https://economysea.withgoogle.com [Accessed 1 February 2022].

16. Hamzah, L. M. & Agustien, D. (2019) Pengaruh Perkembangan Usaha Mikro, Kecil, dan MenengahTerhadap Pendapatan Nasional Pada Sektor UMKMdi Indonesia. Jurnal Ekonomi Pembangunan (JEP) 8(2), 127-135.

17. Holdsworth, J. and Apeh, E., 2017. An Effective Immersive Cyber Security Awareness Learning Platform for Businesses in the Hospitality Sector. 2017 IEEE 25th International Requirements Engineering Conference Workshops (REW),.

18. ITS, 2021. Keamanan Siber - Departemen Teknologi Informasi. [online] Departemen Teknologi Informasi. Available at: https://www.its.ac.id/it/id/keamanan-siber/ [Accessed 20 November 2021].

19. Kabanda, S., Tanner, M. & Kent, C. (2018) Exploring SME cybersecurity practices in developing countries. Journal of Organizational Computing and Electronic Commerce, 28(3), 269-282.

20. Kemp, S. (2017) DIGITAL 2017: ASIA-PACIFIC REGIONAL OVERVIEW. Available online: https://datareportal.com/reports/digital-2017-apac-regional-overview [Accessed 1 February 2022].

21. Kirlappos, I. and Sasse, M., 2012. Security Education against Phishing: A Modest Proposal for a Major Rethink. IEEE Security & Privacy Magazine, [online] 10(2), pp.24-32. Available at: <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6109230>.

22. Kissel, R., 2013. Glossary of Key Information Security Terms. Gaithersburg: National Institute of Standards and Trade, pp.17, 106, 185.

23. Kleist, V. F. (2018) An Interview with Maria Vello: Chief Executive Officer of the Cyber Defence Alliance (CDA). Journal of Global Information Technology Management, 21(4), 301-305.

24. Lallie, H., Shepherd, L., Nurse, J., Erola, A., Epiphaniou, G., Maple, C. and Bellekens, X., 2021. Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. Computers & Security, 105, p.102248.

25. Lee, I., 2021. Cybersecurity: Risk Management framework and investment cost analysis. Business Horizons, 64(5), pp.659-671.

26. Mamonov, S. and Benbunan-Fich, R., 2018. The impact of information security threat awareness on privacy-protective behaviors. Computers in Human Behavior, [online] 83, pp.32-44. Available at: <https://reader.elsevier.com/reader/sd/pii/S0747563218300347?token=D243866CEF7F2D029EB710314E73AE03B536E40C2E6F134AE52EF3C2E6E80C8747F5062C5509AE5EDFAE422AAF508D88&originRegion=eu-west-1&originCreation=20211118112841> [Accessed 18 November 2021].

27. NCSC, 2020. Cyber Security Small Business Guide. London: National Cyber Security Centre, p.15.

28. NCSC, 2021. What Is cyber security?. [online] Ncsc.gov.uk. Available at: https://www.ncsc.gov.uk/section/about-ncsc/what-is-cyber-security [Accessed 20 November 2021].

29. Ponsard, C., Grandcalaudon, J. & Bal, S. (2019) Survey and Lessons Learned on Raising SMEAwareness about Cybersecurity, 5th International Conference on Information Systems Security and Privacy (ICISSP 2019). CETIC Research Centre, Charleroi, Belgium: SCITEPRESS – Science and Technology Publications, Lda.

30. Rahim, N., Hamid, S., Mat Kiah, M., Shamshirband, S. and Furnell, S., 2015. A systematic review of approaches to assessing cybersecurity awareness. Kybernetes, 44(4), pp.606-622.

31. Sabillon, R., Cavaller, V., Cano, J. and Serra-Ruiz, J., 2016. Cybercriminals, Cyberattacks and Cybercrime Privacy, security and control.

32. Saravanan, A. and Bama, S., 2019. A Review on Cyber Security and the Fifth Generation Cyberattacks. Oriental Journal of Computer Science and Technology, [online] 12(2), pp.50-56. Available at: <http://dx.doi.org/10.13005/ojcst12.02.04> [Accessed 2 May 2022].

33. Saunders, M., Lewis, P. and Thornhill, A., 2019. Research methods for business students. 8th ed. Harlow: Pearson Education Limited, pp.651-657.

34. Suartana, I., Eka Putra, R., Bisma, R. and Prapanca, A., 2022. Pengenalan Pentingnya Cyber Security Awareness pada UMKM. Jurnal Abadimas Adi Buana, 5(02), pp.197-204.

35. Tianfield, H., 2016. Cyber Security Situational Awareness. In: 2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData). [online] Glasgow: IEEE, p.782. Available at: <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7917193> [Accessed 22 November 2021].

36. Wang, Y., Zhou, A., Liao, S., Zheng, R., Hu, R. and Zhang, L., 2021. A comprehensive survey on DNS tunnel detection. Computer Networks, 197, p.108322.

37. Yu, B., Olumofin, F., Smith, L. and Threefoot, M., 2016. Behavior Analysis based DNS Tunneling Detection and Classification with Big Data Technologies. Proceedings of the International Conference on Internet of Things and Big Data,