Received 1 June 2023, accepted 21 June 2023, date of publication 7 July 2023, date of current version 16 August 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3293062

RESEARCH ARTICLE

Digital Risk Assessment Framework for Individuals: Analysis and Recommendations

SUADAD MUAMMAR[1,2], (Member, IEEE), DINA SHEHADA[1], (Member, IEEE), AND WATHIQ MANSOOR[1], (Senior Member, IEEE)

[1]Department of Engineering and IT, University of Dubai, Dubai, United Arab Emirates
[2]Department of Computer Science, British University in Dubai, Dubai, United Arab Emirates

Corresponding author: Suadad Muammar (smuammar@ud.ac.ae)

ABSTRACT As individuals increasingly engage with the digital landscape, they face a multitude of risks associated with their online activities and the security of their personal information. Individuals seek guidance in balancing the benefits and risks of the digital transformation. To effectively mitigate these risks, it is essential to establish a comprehensive Digital Risk Assessment Framework tailored to individual users. In this research, an a interpretive study have been carried out to propose a novel Digital Security Management Framework. The main contribution of this study is providing a novel approach by examining the recent recorded threats against individuals, quantifying these threats, and proposing a novel digital risk framework detailing the list of threats and the corresponding risk treatment options tailored for individuals. The scenario of the case study is a family that use personal computers to access banking and investment accounts online, engage in online shopping and also frequently use social media to share artwork and opinions. 17 types of digital risks were identified and the probability of loss and impact of each risk have been quantified using Bernoulli distribution f(L;p). The quantified values were used to prioritise mitigation measures. According to the results, and the proposed framework, suitable treatment option(s) was recommended for each risk. The results show that online scams present the biggest financial risk to individuals, that security incidents present a moderate risk, and that communication-based harms (e.g. bullying and radicalization) are difficult to quantify.

INDEX TERMS Digital risk assessment, cybercrime; online activity, framework, digital risk treatment options, digital security threats.

I. INTRODUCTION

In today's digital age, individuals are increasingly exposed to a wide range of risks associated with their online activities and the security of their personal information. The proliferation of technology and the inter-connectedness of digital platforms have opened new avenues for cyberthreats, privacy breaches, and identity theft. According to the latest statistics from Statista,[1] more than five billion people around the world use the Internet. Many of these users connect to the Internet in their homes through broadband Internet services using their personal computers (PCs) and mobile phones for their personal and business needs, such as accessing the Web, communicating with friends and family, accessing online trading platforms, shopping online, and working from home.

Internet-connected devices have undoubtedly added convenience to our lives, however, they have also introduced a wide range of threats and vulnerabilities. In 2018, the Internet Crime Complaint Center (IC3) published that estimated the accumulated total global loss since 2013 to be $12.5 billion [1] from 78,617 incidents [2];

In 2021, research conducted online by The Harris Poll on behalf of NortonLifeLock revealed that approximately one in five individuals had fallen victim to a scam such as clicking on a fraudulent package notification link in the past 12 months among 10,030 adults (aged 18+) in 10 countries

The associate editor coordinating the review of this manuscript and approving it for publication was Jemal H. Abawajy.

[1] https://www.statista.com/statistics/617136/digital-population-worldwide/

[3]. In the same study, 35% of the respondents mentioned that they did not know how to protect themselves from cybercrime.

Educating users about digital risks and available protection measures is no less important for homes than for businesses.

While a cyberattack on a company may cause financial losses or disrupt services, online scams and attacks against individuals can lead to financial ruin and emotional trauma [4], [5]. The potential for digital harm motivates a structured approach. Risk management theory has been prescribed for companies to address cybersecurity risks [6], [7], [8], [9]. This seems equally applicable for home users given they face not only cybersecurity risk, but also privacy and information based harms.

The cost of digital risks for end users can be significant and can have a range of negative impact on individuals and their lives. It is important for end users to be aware of these risks and to take appropriate measures to protect themselves against them. To effectively mitigate these risks, it is essential to establish a comprehensive digital risk assessment framework tailored to individual users. The objective of this study is to provides a clear digital risk assessment framework to answer the below research question: **What types of digital security threats do individuals commonly encounter, and what security treatment options can be used to mitigate these threats?**

The main output of our research paper is to conduct a digital risk assessment for a hypothetical family (more details in the next section), which serves multiple purposes. First, it can identify risks and effective mitigation measures for families in a similar situations to our hypothetical scenario. Second, the gaps in our risk assessment serve to motivate and guide future work. For example, cybersecurity experts, such as engineers can design mitigation measures that prevent the most costly harms. Academicians can use the proposed framework as a reference for their own projects, or further investigations. In general, risk assessment practices and frameworks can help experts in identifying, assessing, and prioritizing cybersecurity risks specific to organization or industry.

The main contribution of this study is: providing a novel approach to examine the recent recorded threats against individuals, quantifying these threats, and proposing a unique digital risk framework tailored to individuals detailing the list of threats and the corresponding risk treatment options. To the best of out knowledge this is the first digital risk framework dedicated to address digital risks for individuals.

In the next section, Section II, the related work is discussed. The rest of the paper is structured as follows: Section III highlights the proposed methodology, Section IV identifies potential risks. Section V quantifies the likelihood and impact of each risk and provides analysis of the results. Section VI provides a discussion and summary of the results including the proposed digital risk management framework. Section VII concludes the paper findings. Final, Section VIII highlights the limitation and future work.

II. RELATED WORK

The work in [10] reviews the evidences provided by victim surveys in order to provide a rough estimate for the personal crime prevalence of the main types of cybercrime. The study analyzes the percentage based on the number of victims of cybercrimes that occurred in Europen from 2009 to 2016 based on six categories. The work in [11] quantifies the impact of different threats. It investigates if social-reporting techniques used to generate estimates of physical crime prevalence can be generalized to cybercrimes. In addition, the work in [1] proposed a framework for analyzing the costs of cybercrimes. The work in [12] presented three taxonomies based on an extensive review of the social media community guidelines and previous works.

The work in [13] presented an investigation online cybersecurity and privacy behaviors and security and privacy practices of older adults in urban India, and suggested the collaborative behaviours enacted by different members of the family for protection from such type of threats. Reference [14] addressed the privacy issues at the level of individuals and developed a model to study how the consumers' concerns about privacy, security and trust in addition to their risk beliefs can impact their engagement in e-commerce transactions. Moreover [15] focused on the concept of social cybersecurity and how individuals can be compromised. The work in [16] propose a model for online retail industry to have a clear understanding of the factors influencing online consumers' intentions toward online purchase across gender. Results showed that female customers showed a higher level toward the security of online transactions compared to male.

While some of the related works discussed the threats and categorized them [10], [12]. While others discussed the impact and cost of these threats [1], [11]. Nonetheless, these works did not address the recommended measures for each threat. Moreover, previous studies have focused on addressing different aspect of cybersecurity such as information privacy, and identifying digital security threats in business or industry fields, this paper provides a detailed analysis of the different threats faced by individuals. The different threats used in this study were published in government reports [17], [18], [19], [20] and academic papers [1], [10], [11]. This study takes a novel approach by examining the recent recorded threats against individuals, quantifying these threats, and propose a unique digital risk framework detailing the list of threats and the corresponding risk treatment options. To the best of out knowledge this is the first digital risk framework dedicated to address digital risks for individuals.

III. METHODOLOGY

In this section the hypothetical family scenario, risk assessment and data sources used in our study are explained in details. Figure 1 shows the proposed methodology.

A. HYPOTHETICAL FAMILY

Our family uses connected mobile devices and laptops without any Internet of Things (IoT) devices involved. We did not consider IoT devices because the attack surface expands to include car accidents (smart cars), home burglary (smart homes), medical issues (smart medicine) and so on. Some individuals access their banks and investment accounts online. They also frequently engage in online shopping on different e-commerce websites. Moreover, some also used social media to share artwork and political opinions, which has led them to many political forums.

B. RISK ASSESSMENT

Our digital risk assessment first identified potential harms. The probability and loss of each was quantified. The quantified values were used to rank the threats into high, medium, and low. Finally, a suitable treatment option was recommended for each threat. We tried to identify specific protection measures. Reduction, transfer, acceptance, and avoidance are the four main risk treatment options [21]. The selection of appropriate risk treatment options was based on Risk Impact Grid [21], [22] which is a well-known risk management tool based on the probability of occurrence and the severity or the potential loss of the risk. One treatment option or more can be applied to a single risk to manage the likelihood or impact of the risk. Figure 2 shows the four treatment options, and their relationship with the loss and probability. A description of each risk treatment option is presented below:

1) ACCEPTANCE

Understanding the risk and its consequences and consciously deciding to accept it is known as risk acceptance [21]. The acceptance treatment option can be considered if both the probability and impact of the risk are low, as shown in Figure 2. With this strategy, individuals continue to behave normally but are conscious of the risk. This involves accepting that technology cannot be 100% secure, and there is always a level of acceptance. This option is typically applied when further risk reduction or transfer would be more expensive than simply accepting the risk.

2) REDUCTION

Risk reduction is an important and common strategy that includes various security measures to mitigate the likelihood of risk occurrence and its impact. Reduction is rarely fully effective, but it helps to reduce the risk to a level such that it can be accepted [21]. Common security measures to be considered for reducing the probability of threats are access control (e.g. passwords and MFA), network security (e.g. firewalls and TLS), and device security (e.g. anti-virus and security updates). Reducing the impact of loss is typically done by creating and practicing crisis response plans.

3) TRANSFER

Risk transfer involves shifting liability related to a particular activity to another party [21], [23]. Risk is most commonly transferred to an insurer, typically low likelihood but high impact events, as shown in Figure 2. Other examples of risk transfer include platforms covering the cost of retail fraud when goods are not shipped or banks restoring funds after fraudulent withdrawals.

4) AVOIDANCE

In some cases, individuals should stop activities that cause high exposure to risks, for which risk reduction is ineffective and insurance is not available at a reasonable cost. Risk avoidance can ranges from subtle to dramatic. An extreme avoidance strategy would be to close online bank accounts and stop shopping online, relying on cash payments at brick-and-mortar stores. More subtle cases involve withdrawing from specific activities, such as e-commerce websites that do not communicate via HTTPS. Similarly, it is advisable to avoid investment opportunities presented via email, but one might still feel comfortable doing so via a reputable online investment broker.

C. SECONDARY DATA SOURCES

The cybercrimes and threats used in this study were published in government reports [17], [18], [19], [20] and academic papers [1], [10], [11]. The threats were experienced by individuals in different countries, such as Australia, USA, and Switzerland. These threats were categorized into four different categories (explained in details in the next section) to make it easier for the individual to identify the threat and the recommended measures.

IV. RISK IDENTIFICATION

Table 1 presents the digital risks experienced by individuals in different countries. From academic papers [1], [10], [11] and government reports [17], [18], [19], [20], we identified the following:

- Online sales fraud: This involves cases where goods are not delivered, are counterfeit, or are not as advertised [24]. In one example, goods or services are shipped and payment is never rendered (non-payment). Alternatively, a payment is sent, and goods or services are never received or are of low quality (non-delivery) [17]. This can happen when a scammer requires a victim to use an unexpected payment mechanism (gift card, Bitcoin) after being paid and never delivers the products [11].
- Overpayment: This may occur when a scammer overpays for something a victim is selling online and then asks for an extra amount to be refunded after the victim discovers that the original payment method is invalid, such as a stolen credit card [11], [17].
- Real estate scam: Loss of funds from real estate investment or fraud involving a rental or timeshare property [17].
- Technical support scam: This threat involves a criminal claiming to provide technical support or services in order to defraud unwitting individuals. Criminals may act as support representatives and offer to resolve issues

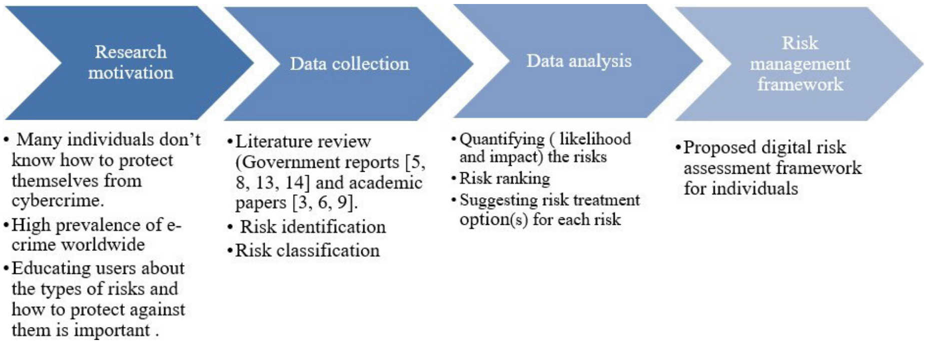
Research motivation
Data collection
Data analysis
Risk management framework
• Many individuals don't know how to protect themselves from cybercrime.
• High prevalence of e-crime worldwide
• Educating users about the types of risks and how to protect against them is important .
• Literature review (Government reports [5, 8, 13, 14] and academic papers [3, 6, 9].
• Risk identification
• Risk classification
• Quantifying (likelihood and impact) the risks
• Risk ranking
• Suggesting risk treatment option(s) for each risk
• Proposed digital risk assessment framework for individuals

FIGURE 1. Proposed methodology.

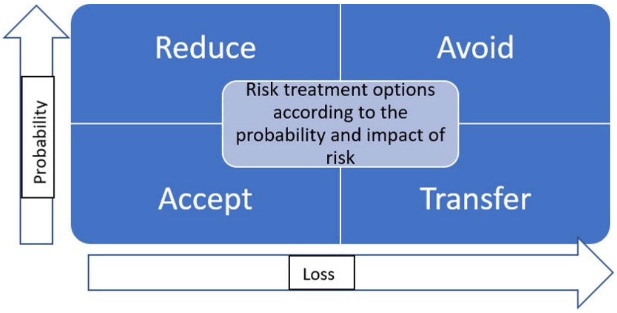
Reduce
Avoid
Risk treatment options according to the probability and impact of risk
Accept
Transfer
Probability
Loss

FIGURE 2. Risk impact grid treatment options.

such as a compromised e-mail or a software licence renewal [17].

- Identity theft: Identity theft is the deliberate use of someone else's identity, usually as a method to gain financial advantage or obtain credit and other benefits in the other person's name. Identity theft occurs when someone uses another person's personal identifying information, such as their name, identification number, or credit card number, without their permission, to commit fraud or other crimes [10].
- Personal data breach: This is a leak/spill of personal data released to a party who was not intended to have access to the data. It is a security incident in which an individual's sensitive, protected, or confidential data are copied, transmitted, viewed, stolen, or used by an unauthorised individual [17].
- Malware: Malicious software (i.e. malware) is a term used to describe programs such as ransomware, computer viruses, and rootkits with hidden functionality that negatively impacts infected computers. For example, ransomware, is a type of malware designed to block access to a computer system or to files stored on a computer until money (the ransom) is paid. Software or code intended to damage, disable, or copy itself onto a computer and/or computer systems can have a detrimental effect or destroy data [17].
- Spoofing: This occurs when contact information (phone number, e-mail, and website) is deliberately falsified to mislead and appears to be from a legitimate source. Spoofing is often used in connection with other types of crime [17].
- Cyberbullying: Cyberbullying refers to bullying (inappropriate or harassing messages, texts, and pictures) that occurs using electronic technology. Cyberbullying messages and images are often posted anonymously and can be distributed quickly to a wide audience [10]. This includes child sexual abuse material, incitement of racial hatred, racism, xenophobia, negative comments about physical appearance and so on [18]. Harassment and bullying involves, which can involve targeted harassment or a perpetrator inciting other people to do so, sending threatening messages, and establishing malicious unsolicited contact and making threats [12].
- Copyright: Copyright and counterfeit involves the illegal theft and use of others' ideas, inventions, and creative expressions, which is called intellectual property and includes trade secrets, proprietary products, and movies, music, and software [17]. Copyright law gives authors, artists, and inventors the exclusive rights to their respective writings and artwork and discoveries [25].

These common threats can be categorised into four main categories which are:

- Online shopping risks: Many individuals, including family members at home, rely on technology to buy and/or sell products and services through online platforms that allow them to pay for goods. Online shopping, the inability to inspect retail before purchase, and a lack of direct contact between buyers and sellers may cause online fraud [10].
- Online investment risks: Individuals believe they are investing their money through different online platforms, such as banks, real estate, and other businesses. In reality, the investments are fraudulent in various ways ranging from not being as advertised through to not existing.
- Generic threats for both online shopping and investment digital security: This category of cybercrime includes threats that can lead to online shopping fraud or online investment fraud. For example, banking fraud can result from malware or other modes of attack [24].

TABLE 1. Common cybersecurity threats.

	Threats	References
Online shopping digital security threats	Sales fraud: non-payment, non-delivery	[1, 10, 11, 17]
	Credit card fraud/banking scam	[1, 11, 17]
	Overpayment	[1, 10, 11, 17–20]
	Re-shipment	[17]
Generic threats for online shopping and investment digital security	Identity theft	[1, 10, 11, 17–20]
	Personal data breach	[1, 10, 11, 17–20]
	Malware (ransomware, virus)	[1, 10, 11, 17–20]
	Phishing	[1, 10, 11, 17–20]
	Extortion	[1, 10, 11, 17–20]
	Advance fee	[17, 18]
	Confidence fraud	[17]
	Spoofing	[11, 17]
Investment digital security threats	Real estate scam	[17]
	Technical support scam	[17, 18]
	Investment scam	[17, 18]
Threats on social media (opinion and artwork sharing)	Cyberbullying	[1, 10, 11, 17]
	Copyright	[17]

- Social media harms: Abusive attacks include intimate partner violence, anonymous peers breaking into a target's account to leak personal communication and photographs, and coordinated bullying and sexual harassment campaigns involving tens of thousands of attackers. In a 2017 survey conducted by Pew, 40% of people reported experiencing varying degrees of harassment and bullying online. Attacks in this category include bullying, trolling (e.g. intentionally provoking audiences with inflammatory remarks), threats of violence, and sexual harassment. Toxic content can be used to violate availability, preventing victims from properly taking advantage of an online community or even forcing them to leave it [26].

V. RESULTS & ANALYSIS

A. QUANTIFYING LIKELIHOOD AND IMPACT OF DIGITAL RISK

To assess each digital risk, we quantify the likelihood and impact of each threat. This will help evaluate the potential impact of threats, prioritise the mitigation measures, and provide recommendations to family members. To measure risk, it is necessary to choose a model to specify the relationship among risk factors, including the resource value, vulnerability effect, threat impact, and threat likelihood [21]. Several methods can be used to quantify the likelihood and impact of digital risk.

In this study, we use a Bernoulli distribution $f(L;\ p)$, which is a binomial distribution, to estimate the risk of a given threat (X) that may occur with probability (P) and its impact in terms of financial loss (L). Although the threats were collected from different sources, such as government reports [17], [18], [19], [20] and academic papers [1], [10], [11], we utilize the most recent IC3 report [10] published in 2021 to obtain consistent data on the total loss and number of victims who experienced each of the threats listed above. We estimate the likelihood of an event by dividing the total number of victims by the size of the population (US population: 331900000) and then based on digital users (digital population of the US: 302280000) to obtain more accurate estimations. The average loss is estimated by dividing the total financial loss by the number of cases. he formula used to measure the risk of each identified threat are as follows:

$$Risk = probability\ of\ loss\ event(P) \times magnitude\ of\ loss(L) \tag{1}$$

$$Risk = (\frac{\#\ of\ reported\ cases}{population}) \times (\frac{financial\ loss}{reportedcases}) \tag{2}$$

B. RISK TREATMENT RANKING

Table 2 shows the results after quantifying the risks. Risk evaluation is the process of rating risk exposures on a scale to determine the significance of each risk and then select the appropriate risk treatment option(s) to manage the risks and address them appropriately [21]. We quantify a risk by multiplying its probability and loss, and the following scale ranking is used for probability and loss. The median of the loss was found to be 6909 which was used to set the ranges for the high, medium, and low ranks as follows: The risk's impact (loss) is:

- high (red): if the loss is $\geq$ 13800,
- medium (yellow): if the loss is $\geq 6909(median)$,
- low (green): if the loss is <6909.

The probability is:

- high (red): if the probability is $\geq$ 0.00099,
- medium (yellow): if the probability is $\geq$ 0.000099,
- low (green): if the probability is <0.0000099.

Table 3 shows the rank of each threat according to the applied methodology.

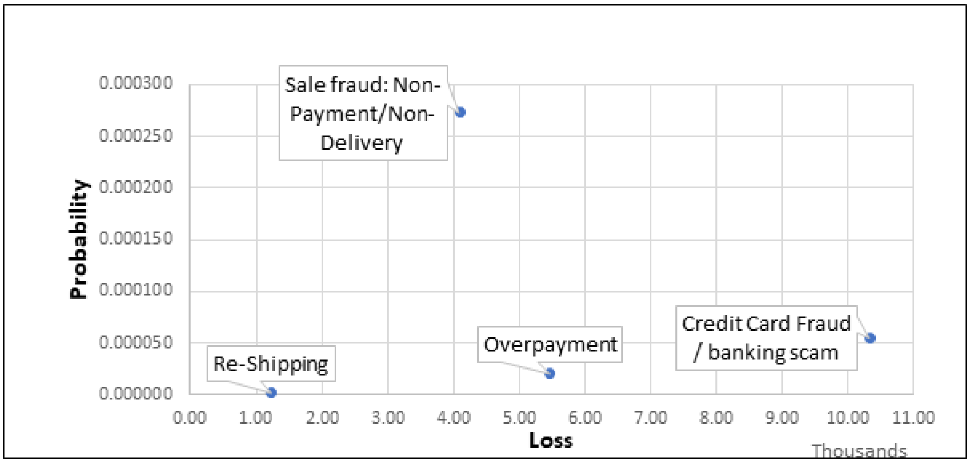

FIGURE 3. Digital risks associated with online shopping.

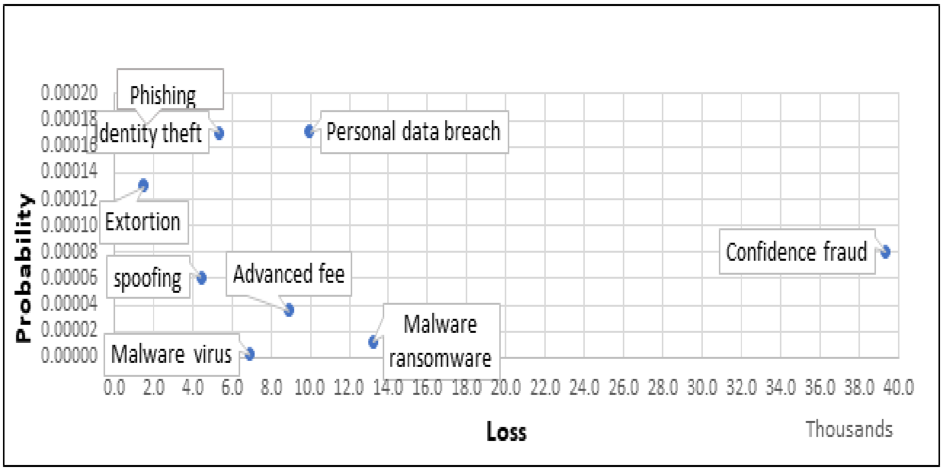

FIGURE 4. Digital risks associated with investment.

C. RISK TREATMENT RECOMMENDATIONS

For each risk, we will suggest a risk treatment option(s) according to the previously discussed methods. As explained in the methodology section, we assigned scale to the likelihood (probability) and impact (loss) of threats to suggest a suitable security option(s) for each risk. For example, identity theft, the likelihood of this risk occurrence is high 0.000171 (between 0.00001 and 0.000199) and the impact of it is considerably low to medium 5389.8 (between 0 and 6909). The best security treatment option in this case is risk reduction.

1) ONLINE SHOPPING SECURITY RISKS

Sales fraud (non-payment/non-delivery): As shown in Table 3 and Figure 3, the probability of this risk is high, and the loss is low-to-medium (loss: 4091.9, probability: 0.000273). This suggests risk reduction is appropriate, which likely consists of reading through reviews and conducting due dilligence on the seller. In addition, the transfer option could be used by purchasing with a credit card and asking the bank to charge back if sales fraud occurs. All of these methods incur a time cost that should not be ignored.

Credit card fraud/banking scam: As shown in Table 3 and Figure 3, the probability of this risk is medium, and the loss is medium as well (loss: 10328.3, probability: 0.000055). This suggests any treatment could be appropriate depending on which are available. In some cases banks may refund fraudulent losses, but this varies by country and banks often make it difficult [27]. Typically banks will require certain security procedures to follow, which also help to reduce the risk.

Overpayment: As shown in Table 3 and Figure 3, the probability of this risk is high, and the loss is low (loss: 5469.5, probability: 0.000020). In this case, a risk-reduction treatment option is recommended to avoid dealing with untrustworthy businesses.

Re-shipping: As shown in Table 3 and Figure 3, both the probability and impact of this risk are low (loss: 1223.8, probability: 0.000002). In such cases, individuals may accept the risk with some consciousness.

2) ONLINE INVESTMENT DIGITAL SECURITY RISKS

Real estate/rental scam: As shown in Table 3 and Figure 4, the probability of this risk is medium, and the loss is high (loss:

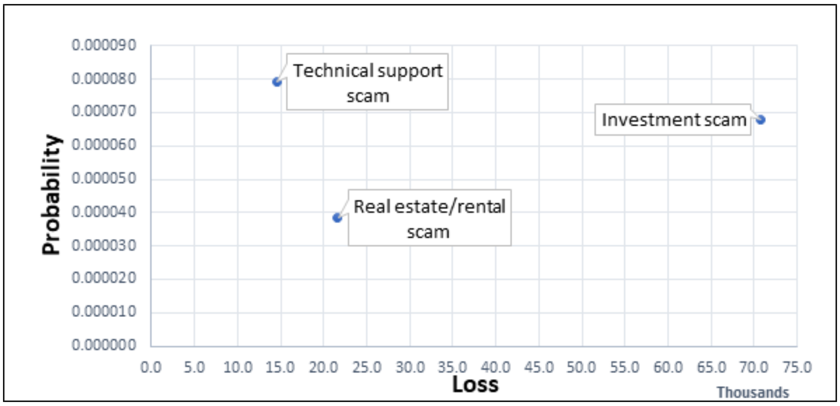

FIGURE 5. Digital risks associated with online shopping and investment.

TABLE 2. Quantifying the likelihood and impact of risk.

Threats categories	Crime type	Number of victims	Financial loss	Probability (based on Population)	Loss	Risk (based on Population)	Probability (based on Digital users)	Risk (based on digital users)
Online Shopping digital security threats	Sale fraud: Non-Payment/Non-Delivery	82,478	337.49M	0.000249	4091.9	1.017	0.000273	1.116
	Credit Card Fraud / banking scam	16,750	173.00M	0.000050	10328.3	0.521	0.000055	0.572
	Overpayment	6,108	33.41M	0.000018	5469.5	0.101	0.000020	0.111
	Re-Shipping	516	0.63M	0.000002	1223.8	0.002	0.000002	0.002
Generic threats for online shopping and investment digital security threats	Identity theft	51,629	278.27M	0.000156	5389.8	0.838	0.000171	0.921
	Personal data breach	51,829	517.02M	0.000156	9975.5	1.558	0.000171	1.710
	Malware ransomware	3,729	49.21M	0.000011	13196.0	0.148	0.000012	0.163
	Malware virus	810	5.60M	0.000002	6909.7	0.017	0.000003	0.019
	Phishing	323,972	44.21M	0.000976	136.5	0.133	0.001072	0.146
	Advanced fee	11,034	98.69M	0.000033	8944.5	0.297	0.000037	0.326
	Extortion	39,360	60.58M	0.000119	1539.1	0.183	0.000130	0.200
	Confidence fraud	24,299	956.04M	0.000073	39344.8	2.881	0.000080	3.163
	spoofing	18,522	82.17M	0.000056	4436.3	0.248	0.000061	0.272
Investment digital security threats	Real estate/rental scam	11,578	250.33M	0.000035	21621.0	0.754	0.000038	0.828
	Technical support scam	23,903	347.66M	0.000072	14544.5	1.047	0.000079	1.150
	Investment scam	20,561	1455.94M	0.000062	70810.9	4.387	0.000068	4.817
Threats of using social media (artwork sharing)	IPR/copyright and counterfeit	4,270	16.37M	0.000013	3832.6	0.05	0.000014	0.054

21621.0, probability: 0.000038). In this case, a risk avoidance treatment option is recommended. Instead individuals should interact with established firms who are more likely to be regulated and also have a reputation to protect.

Technical support scam: As shown in Table 3 and Figure 4, the probability of this risk is medium, and the loss is high (loss: 14544.5, probability: 0.000079). In this case, a risk avoidance treatment option is recommended to avoid dealing with untrustworthy businesses. This means being skeptical whenever someone contacts the individual about technology support, which likely requires some awareness training.

Investment scam: As shown in Table 3 and Figure 4, the probability of this risk is medium, and the loss is high (loss: 70810.9, probability: 0.000068). In this case, a risk avoidance treatment option is recommended. Much like with real estate scams, individuals should find established stock brokers. This involves ignoring cold emails promising supposed investment opportunities.

3) GENERIC THREATS FOR BOTH ONLINE SHOPPING AND INVESTMENT DIGITAL SECURITY

Identity theft, extortion, spoofing, phishing: As shown in Table 3 and Figure 5, the probability of each of these risks is medium-to-high, and the loss of each risk is low (loss: 5389.8, probability: 0.000171), (loss: 1539.1, probability: 0.000130), (loss: 4436.3, probability: 0.000061), and (loss: 136.5, probability: 0.001072). In this case, the risk-reduction treatment option is ideal. Interestingly, there are personal identity insurance products available [28], but the low impact of thefts calls into question how valuable these products are.

Personal data breach: As shown in Table 3 and Figure 5, the probability of this risk is high, and the loss is medium (loss: 9975.5, probability: 0.000171). In this case, a riskreduction treatment option is recommended to avoid dealing with untrustworthy businesses.

Malware ransomware and confidence fraud: As shown in Table 3 and Figure 5, the probability of each of these risks is medium, and the loss is high (loss: 13196.0, probability: 0.000012). In this case, a risk-reduction treatment option is recommended to avoid dealing with untrustworthy businesses. In addition, the transfer option should be considered to eliminate loss if it occurs. Avoidance treatment options should also be considered.

Malware virus: As shown in Table 3 and Figure 5, this risk probability is low, and the loss is medium (loss: 6909.7, probability: 0.000003). In this case, a risk reduction treatment

TABLE 3. Risk ranking.

Threats categories	Crime type	Number of victims	Financial loss	Probability (based on Population)	Loss	Risk (based on Population)	Probability (based on Digital users)	Risk (based on digital users)
Online Shopping digital security threats	Sale fraud: Non-Payment/Non-Delivery	82,478	337.49M	0.000249	4091.9	1.017	0.000273	1.116
	Credit Card Fraud / banking scam	16,750	173.00M	0.000050	10328.3	0.521	0.000055	0.572
	Overpayment	6,108	33.41M	0.000018	5469.5	0.101	0.000020	0.111
	Re-Shipping	516	0.63M	0.000002	1223.8	0.002	0.000002	0.002
Generic threats for online shopping and investment digital security threats	Identity theft	51,629	278.27M	0.000156	5389.8	0.838	0.000171	0.921
	Personal data breach	51,829	517.02M	0.000156	9975.5	1.558	0.000171	1.710
	Malware ransomware	3,729	49.21M	0.000011	13196.0	0.148	0.000012	0.163
	Malware virus	810	5.60M	0.000002	6909.7	0.017	0.000003	0.019
	Phishing	323,972	44.21M	0.000976	136.5	0.133	0.001072	0.146
	Advanced fee	11,034	98.69M	0.000033	8944.5	0.297	0.000037	0.326
	Extortion	39,360	60.58M	0.000119	1539.1	0.183	0.000130	0.200
	Confidence fraud	24,299	956.04M	0.000073	39344.8	2.881	0.000080	3.163
	spoofing	18,522	82.17M	0.000056	4436.3	0.248	0.000061	0.272
Investment digital security threats	Real estate/rental scam	11,578	250.33M	0.000035	21621.0	0.754	0.000038	0.828
	Technical support scam	23,903	347.66M	0.000072	14544.5	1.047	0.000079	1.150
	Investment scam	20,561	1455.94M	0.000062	70810.9	4.387	0.000068	4.817
Threats of using social media (artwork sharing)	IPR/copyright and counterfeit	4,270	16.37M	0.000013	3832.6	0.05	0.000014	0.054

option is recommended to avoid dealing with untrustworthy businesses or downloading e-mail attachments if they are not expected. In addition, the transfer option should be considered to eliminate loss if it occurs.

Advance fee: As shown in Table 3 and Figure 5, for this risk, both the probability and loss are medium (loss: 8944.5, probability: 0.000037). In this case, a risk-reduction treatment option is recommended to avoid dealing with untrustworthy businesses. In addition, avoidance treatment options should be considered.

4) SOCIAL MEDIA THREATS

Copyright: The probability of this risk is medium-to-high, and the loss is low-to-medium. We recommend the acceptance treatment option if the impact is low and the transfer option if the cost is medium and the probability is medium-to-high (loss: 3832.6, probability: 0.000014).

Cyberbullying: The risk reduction, risk avoidance, and risk transfer treatment options should be considered to protect teenagers/children from this risk and eliminate its impact if it occurs. According to Kaspersky4, the best foundation for protecting against cyberbullying is parents talking with their children about what is going on in their lives online and in real life and how to stand up to bullies. In addition, the use of the Internet by children should be limited and monitored; many cybersecurity suites and specialised apps can be used to filter out abusive content. Insurance companies help families deal with this risk, and families should report such cases to insurers. Additionally, families should consider avoidance options and prevent their children from accessing websites that present such risks.

VI. DISCUSSION & SUMMARY

A. DIGITAL RISK ASSESSMENT RELATED TO ONLINE SHOPPING

Sales fraud, credit card fraud, banking scams, overpayment, re-shipping, identity theft, extortion, spoofing, phishing, personal data breaches, malware ransomware and confidence fraud, malware viruses, and advance fees are the digital risks associated with buying and selling goods through online platforms such as e-commerce websites. One or more risk treatment options, as described in the previous section, are recommended for each risk according to the probability of the risk and its impact. Digital security measures are recommended to families for this category of risks, e.g. installing an Internet security suite on all computers and making sure to update this program among the other programs on the computers, educating family members to increase their awareness of the risks associated with using services on the Internet, reporting threat incidents, and in some cases, risk transfer should be considered to eliminating the impact of risk, for example, when goods are purchased and not delivered.

B. DIGITAL RISK ASSESSMENT RELATED TO ONLINE INVESTMENT

Real estate/rental scams, technical support scams, investment scams, identity theft, extortion, spoofing, phishing, personal data breaches, malware ransomware and confidence fraud, malware viruses, and advance fees are the digital risks associated with online investment through online platforms such as bank websites and real estate websites. Digital security measures are recommended to families for this category of risks, e.g. installing an Internet security suite on all computers and making sure to update this program among the other programs on the computers, educating family members to increase their awareness of the risks associated with using services on the Internet, reporting threat incidents, and eliminating the impact of risk transfer options should be considered in some cases, for example, where goods are purchased and not delivered.

C. DIGITAL RISK ASSESSMENT RELATED TO SOCIAL MEDIA

Copyright and cyberbullying are among the digital risks associated with using social media to share artwork and post

TABLE 4. Proposed digital risk management framework for individuals: analysis and recommendations.

Proposed digital risk management framework for individuals: analysis and recommendations	
Digital risk assessment related to online shopping	
Sales fraud (non-payment/non-delivery)	* Highly recommended: Reduction treatment option such as digital security awareness, Reporting threat incidents, etc. * To be considered: Risk transfer e.g., if goods are not delivered, it is recommended that a party take responsibility for eliminating the impact of such risk.
Credit card fraud/banking scam	* Highly recommended: a combination of risk reduction and transfer treatment options. Examples: software updates, and reporting threat incidents.
Overpayment	* Highly recommended: Reduction treatment option this include: Internet security suite, Digital security awareness, Reporting threat incidents
Re-shipping	* Recommendation: (low probability and loss), individuals may accept the risk with some consciousness.
Online investment digital security risks	
Real estate/rental scam	*Highly recommended (risk with medium probability and high impact): both reduction treatment option, and risk transfer are highly recommended. *To be considered: avoidance treatment option to avoiding dealing with unreputable/trustable entity.
Technical support scam	
Investment scam	
Generic threats for both online shopping and investment digital security	
Identity theft, extortion, spoofing, phishing	* Highly recommended: risk-reduction treatment option is ideal
Personal data breach	* Highly recommended: risk-reduction treatment option is ideal. * To be considered: Risk transfer insurers typically cover the cost of this risk.
Malware ransomware and confidence fraud	* Highly recommended: risk-reduction treatment option is ideal * To be considered: both avoidance treatment option; avoiding dealing with unreputable/trustable entity and risk transfer to eliminate the cost of such risk should be considered.
Malware virus	* Highly recommended: risk-reduction treatment option is ideal * To be considered: Risk transfer insurers typically cover the cost of this risk.
Advance fee	* Highly recommended: risk-reduction treatment option is ideal * To be considered: avoidance treatment options
Social media threats	
Copyright	* Highly recommended: Reduction treatment option this include: digital security awareness, and reporting threat incidents * To be considered: Risk transfer. For example, The protection of artwork by copyright law should also be considered. individuals may accept the risk with some consciousness, Risk acceptance option.
Cyberbullying	* Highly recommended: Reduction treatment option, this include: Internet security suite, Digital security awareness, Reporting threat incidents. * To be considered: Risk transfer, some insurers fight back against bullying and harassment with legal support.

comments or participate in conversations. One or more risk treatment options are recommended for each risk. Several security measures should be considered, e.g. installing Internet security suites that include antiviruses, firewalls, and Internet filters to block untrusted communication and filter content on websites. Moreover, families should keep their personal information private and understand that information can be copied easily online. The protection of artwork by copyright law should also be considered. Finally, family members should be aware of the digital security risks of using social media for their children and discuss these risks with them; for teenagers, parents should discuss possible negative effects of social media on their way of thinking and political leanings.

Table 4 shows a summary for the proposed digital risk management framework for individuals: analysis and recommendations.

VII. CONCLUSION

This paper presents a comprehensive examination of various threats encountered by individuals, drawing from multiple sources including the most recent IC3 report published in 2021. These threats have been classified into four distinct categories, and a digital risk assessment has been conducted to evaluate them. Each threat has been assigned quantified values for probability and loss, allowing for their ranking as high, medium, or low risk. Based on the results, appropriate treatment options have been recommended for each threat. Notably, this paper is the first to offer a digital risk assessment framework specifically tailored for individuals, with the threats sourced from the aforementioned IC3 report published in 2021.

In summary, this study makes a significant contribution to the field of cybersecurity by introducing a proposed framework through a meticulous analysis of 17 global threats faced by individuals, the framework serves as a valuable resource, empowering individuals to proactively anticipate common digital threats and implement corresponding security measures to mitigate them effectively.

VIII. LIMITATION AND FUTURE WORK

The study depends mainly on secondary data collected from Government reports [17], [18], [19], [20] and academic papers [1], [10], [11] to identify the security threats. However, primary data can be useful to validate the proposed framework.

Moreover, quantifying the likelihood and impact of each risk was solely based on the 2021 IC3 report [10], however, it is the most recent source providing statistics on the number of victims and the total cost associated with each listed threat. Obtaining such comprehensive data and statistics for individuals was quite difficult as most statistics focus on threats on business industry rather than individuals.

To overcome this limitation, in the future work we plan to conduct a survey about the impact of digital risks associated with using technologies on individuals. The proposed framework will be tested and evaluated o the newly collected primary data to be validated. Moreover the proposed framework can be extended to include some of the emerging new threats. Another future direction would be, gathering feedback from individuals who have used the proposed framework to provide valuable insights for its improvement.

REFERENCES

[1] R. Anderson, C. Barton, R. Bölme, R. Clayton, C. Gañán, T. Grasso, M. Levi, T. Moore, and M. Vasek, "Measuring the changing cost of cybercrime," in *Proc. Workshop Econ. Inf. Secur.*, 2019, pp. 1–32.

[2] B. W. Clements, "UCC section 4A-207(b) in the age of cybercrime," *Banking L. J.*, vol. 136, p. 302, Jan. 2019.

[3] (2021). *Norton Cyber Safety Insights Report Global Results*. Norton. [Online]. Available: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://now.symassets.com/content/dam/norton/campaign/NortonReport/2021/2021_NortonLifeLock_Cyber_Safety_Insights_Report_Global_Results.pdf

[4] M. Bada and J. R. Nurse, "The social and psychological impact of cyberattacks," in *Emerging Cyber Threats and Cognitive Vulnerabilities*, Amsterdam, The Netherlands: Elsevier, 2020, pp. 73–92.

[5] J. Borwell, J. Jansen, and W. Stol, "The psychological and financial impact of cybercrime victimization: A novel application of the shattered assumptions theory," *Social Sci. Comput. Rev.*, vol. 40, no. 4, pp. 933–954, Aug. 2022.

[6] B. Blakley, E. McDermott, and D. Geer, "Information security is information risk management," in *Proc. Workshop New Secur. Paradigms*, 2001, pp. 97–104.

[7] L. A. Gordon, M. P. Loeb, and T. Sohail, "A framework for using insurance for cyber-risk management," *Commun. ACM*, vol. 46, no. 3, pp. 81–85, Mar. 2003.

[8] S. Romanosky and E. P. Sayers, "Enterprise risk management: Understanding the role of cyber risk," in *Proc. 49th Res. Conf. Commun., Inf. Internet Policy*, 2021, p. 1.

[9] M. Eling, M. McShane, and T. Nguyen, "Cyber risk management: History and future research directions," *Risk Manage. Insurance Rev.*, vol. 24, no. 1, pp. 93–125, Mar. 2021.

[10] C. M. M. Reep-van den Bergh and M. Junger, "Victims of cybercrime in Europe: A review of victim surveys," *Crime Sci.*, vol. 7, no. 1, pp. 1–15, Dec. 2018.

[11] C. Breen, C. Herley, and E. M. Redmiles, "A large-scale measurement of cybercrime against individuals," in *Proc. CHI Conf. Human Factors Comput. Syst.*, Apr. 2022, pp. 1–41.

[12] M. Singhal, C. Ling, P. Paudel, P. Thota, N. Kumarswamy, G. Stringhini, and S. Nilizadeh, "SoK: Content moderation in social media, from guidelines to enforcement, and research to practice," 2022, *arXiv:2206.14855*.

[13] S. Murthy, K. S. Bhat, S. Das, and N. Kumar, "Individually vulnerable, collectively safe: The security and privacy practices of households with older adults," *Proc. ACM Hum. Comput. Interact.*, vol. 5, no. CSCW1, pp. 1–24, Apr. 2021.

[14] A. Gurung and M. K. Raja, "Online privacy and security concerns of consumers," *Inf. Comput. Secur.*, vol. 24, no. 4, pp. 348–371, 2016.

[15] K. M. Carley, "Social cybersecurity: An emerging science," *Comput. Math. Org. Theory*, vol. 26, no. 4, pp. 365–381, Nov. 2020.

[16] C. K. Dewi, Z. Mohaidin, and M. A. Murshid, "Determinants of online purchase intention: a PLS-SEM approach: Evidence from Indonesia," *J. Asia Bus. Stud.*, vol. 14, no. 3, pp. 281–306, Dec. 2019.

[17] *Internet Crime report 2020*, FBI, Washington, DC, USA, 2021.

[18] *Special Eurobarometer 499: Europeans' Attitudes Towards Cyber Security (Cybercrime)*, EU Open Data Portal, European Commission, Brussels, Belgium, 2023.

[19] *ACSC Annual Cyber Threat Report July 2019 to June 2020*, Australian Federal Police, Australian Criminal Intelligence Commission, Canberra City, ACT, Australia, 2020.

[20] M. Lardén, "Criminal justice rehabilitation in Sweden: Towards an integrative model," in *The Palgrave Handbook of Global Rehabil. in Criminal Justice*. Berlin, Germany: Springer, 2022, pp. 559–575.

[21] A. Shameli-Sendi, R. Aghababaei-Barzegar, and M. Cheriet, "Taxonomy of information security risk assessment (ISRA)," *Comput. Secur.*, vol. 57, pp. 14–30, Mar. 2016.

[22] T. Raz and E. Michael, "Use and benefits of tools for project risk management," *Int. J. Project Manage.*, vol. 19, no. 1, pp. 9–17, Jan. 2001. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0263786399000368

[23] D. Woods, I. Agrafiotis, J. R. C. Nurse, and S. Creese, "Mapping the coverage of security controls in cyber insurance proposal forms," *J. Internet Services Appl.*, vol. 8, no. 1, pp. 1–13, Dec. 2017.

[24] D. W. Woods and L. Walter, "Reviewing estimates of cybercrime victimisation and cyber risk likelihood," in *Proc. IEEE Eur. Symp. Secur. Privacy Workshops (EuroS&PW)*, Jun. 2022, pp. 150–162.

[25] C. Shapiro, H. R. Varian, and S. Carl, *Information Rules: A Strategic Guide to the Network economy*. Brighton, MA, USA: Harvard Business Press, 1999.

[26] K. Thomas, D. Akhawe, M. Bailey, D. Boneh, E. Bursztein, S. Consolvo, N. Dell, Z. Durumeric, P. G. Kelley, D. Kumar, D. McCoy, S. Meiklejohn, T. Ristenpart, and G. Stringhini, "SoK: Hate, harassment, and the changing landscape of online abuse," in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2021, pp. 247–267.

[27] R. Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems*. Hoboken, NJ, USA: Wiley, 2020.

[28] D. W. Woods, "Quantifying privacy Harm Via personal identity insurance," *SSRN J.*, pp. 1–15, Dec. 2021.

SUADAD MUAMMAR (Member, IEEE) received the Master of Science degree in information systems from the University of Dubai. She is currently a Lecturer with the College of Engineering and IT, University of Dubai, United Arab Emirates. Her research interests include IT governance, IT platform for community service, green computing, information security, and radio frequency identification (RFID). She has published several research papers in journals and conference proceedings namely; *Journal of International Technology and Information Management*, *International Journal of Business Information Systems*, *International Journal of Information Technology Project Management*, *Education and Information Technologies*, International Conference on Signal Processing and Information Security (ICSPIS), and International Conference on Electronic Devices, Systems and Applications (ICEDSA).

DINA SHEHADA (Member, IEEE) received the M.Sc. degree in computer engineering from Khalifa University, in 2016. She was a Research Associate with the Information Security Research Center (ISRC) and ECE Department for five years. She is currently a Lecturer with the University of Dubai. Her research interests include mobile agent's security, trust evaluation in social networks, formal verification methods, network and information security, machine learning, and the IoT systems.

WATHIQ MANSOOR (Senior Member, IEEE) received the Ph.D. degree in computer engineering from Aston University, U.K. His doctoral work was on the design and implementations of multiprocessors systems and communications protocols for computer vision applications. He is currently a Professor with the University of Dubai. He has an excellent academic leadership experience in well-known universities worldwide. He has published many research articles in the area of intelligent systems, image processing, deep learning, security, ubiquitous computing, web services, and neural networks. His current research interests include intelligent systems and security using neural networks with deep learning models for various applications. He has organized many international and national conferences and workshops. He is a Senior Member of IEEE UAE Section. He has supervised many Ph.D. and undergraduate projects in the field of computer engineering and innovation in business, in addition to co-supervise many postgraduate students through research collaboration with international research groups.