FINANCIAL SERVICES COMMISSION

QUANTIFYING CYBER RISK:

A Cy-VaR Assessment of BIN Attacks on the Barbadian Banking Sector

Thematic Article from the 2024 Financial Stability Report

Quantifying Cyber Risk: A Cy-VaR Assessment of BIN Attacks on the Barbadian Banking Sector

Written by Pinky Joseph[1] and Simone King[2]

Abstract

Cyber risk has emerged as a systemic threat to financial stability, yet it is largely unaccounted for within existing financial stability assessments. This paper contributes to the growing literature on the quantification of cyber risk and provides a novel estimation of potential losses for Barbados, focussing on a Bank Identification Number (BIN) attack scenario. A Value at Risk (VaR) framework is applied and results suggest that annual losses (VaR 95%) could amount to 11 percent of banks' net income and a 3.8 percent increase in operational expenses. Despite these losses, the sector's capital adequacy ratio (CAR) remains well above the minimum regulatory requirement. These findings are valuable for enhancing stress testing frameworks and insightful for banks' cybersecurity investment decisions.

Introduction

Cyberattacks pose a significant threat to the financial sector, underscored by findings from the IMF's Global Financial Stability Report (April, 2024). Based on this report, one-fifth of reported cyberattacks were directed towards the financial sector, with banks as the lead target. Furthermore, a global IT outage in 2024 highlighted the fact that the growth in financial technology has heightened cyber risk exposure. This outage was reported to be due to a faulty update by CrowdStrike, a cyber security company, which affected the operations of Microsoft Windows software globally. Consequently, there were substantial disruptions in the online banking systems, payment systems and customer services of numerous international banks (White, et al., 2024). Rapid growth in automation, storage of sensitive data on online platforms, and the adoption of online banking mechanisms all underscore the urgent need for stronger cybersecurity and cyber risk management.

The rising frequency of cyberattacks and the magnitude of potential losses is concerning for financial stability. Existing studies on cyber risk note that cyberattack losses go beyond the initial financial loss, also encompassing the indirect losses through reputational damage. Erosion of stakeholders' trust and confidence in an institution may materialise as loss of sales, investments and deposits in the case of banks. As such, the quantification of cyber risk losses has gained increasing attention in recent literature, with quantitative analysis mainly founded on a Cyber Value-at-Risk (Cy-VaR) framework. The Cy-VaR concept emerged as part of the World Economic Forum's initiative on cyber resilience and estimates potential cyberattack losses based on assumed frequency of cyberattacks and magnitude of the losses.

Cyber risk quantification is crucial for both financial institutions and central banks. Cybersecurity investments do not directly generate income gains, making it difficult to assess

[1] Pinky Joseph is an Economist in the Research and Economic Analysis Department of the Central Bank of Barbados.
[2] Simone King is a Research Officer in the Research and Economic Analysis Department of the Central Bank of Barbados.
The authors would like to thank the following persons for their helpful comments: Mr. Alwyn Jordan - Deputy Governor, Mr. Anton Belgrave - Director of the Research and Economic Analysis Department and Dr. Saida Teleu - Deputy Director and Chief Research Economist of the Research and Economic Analysis Department.

their return on investment. Instead, the benefits of cyber security investments stem from the prevention of potential cyber risk losses. Without loss estimates, banks – and by extension all institutions- may stall cyber security investments because of their underestimation of the scale and impact of potential losses (Doerr, et al., 2022). Estimated potential loan losses can help inform financial institutions on optimal cyber security investments and guide their provisioning decisions.

From a regulatory standpoint, understanding potential cyber-related losses is equally vital. Capital adequacy is a cornerstone of financial stability assessments, but without robust data on cyber risk exposures, regulators face challenges in accurately evaluating the sector's vulnerability to operational shocks. This paper proposes a simple, forward-looking approach to quantifying cyber risk using publicly available data and case studies, that can be applied by regulators to improve their capital adequacy assessments and financial sector monitoring. Such specialised frameworks are especially important as the Basel III framework is criticised for not handling cyber risk in a granular manner (Peihani, 2022; Krüger & Brauchle, 2021).

Against this background, the aim of this paper is to apply the Cy-VaR framework to generate potential loss estimates, with particular focus on a hypothetical Bank Identification Number (BIN) attack scenario in Barbados. We selected the BIN attack scenario in light of heightened card payments globally (Demirgüç-Kunt, et al., 2022). Barbados presents an interesting case study, as the country strives towards increased digitalisation of payments systems and other financial services which increases the financial sector's exposure to cyber threats.

In terms of the structure, the first six (6) to eight (8) digits of a debit card or credit card is called a BIN, which identifies the card-issuing bank, its country of origin, and other card details (Franklin, Paxson, Perrig, & Savage, 2007). In a BIN attack, fraudsters select a BIN that they wish to target and then apply dedicated software to generate thousands of possible card number combinations. The generated card numbers will be tested at a merchant, usually for small value transactions. Successful card number combinations will then be used for further unauthorised card purchases (ToolCase, 2022; Decisimo, 2024). This scenario is relevant for Barbados, where banks and the two (2) largest credit unions issue Visa and MasterCard ATM cards that use 6- and 8-digit BIN frameworks, respectively (MasterCard, 2017; Visa, 2022; Barbados Today, 2020). After generating the loss estimates, we then evaluate banks' capacity to absorb direct and indirect losses and the impact on liquidity conditions. Both insights will be useful for future development of cyber resilience stress tests. This research contributes to the growing literature on cyber risk quantification, providing first-time quantitative evidence for the Caribbean. Additionally, the paper presents a tractable methodology, supporting replicability and enhancement across other Caribbean countries.

The remainder of this paper is organised as follows. Section 2 provides an overview of cyber risk in the financial sector of Latin America and the Caribbean. Section 3 reviews literature on cyber risk and its drivers, the quantification of cyber risk. Section 4 outlines the methodology, data and scenario. The results are presented in Section 5, followed by concluding remarks in Section 6.

Overview of Cyber Risk in the Financial Sector of Latin America and the Caribbean

According to IBM (2024), the global average cost of a data breach has seen its largest increase since the pandemic from USD $4.5 million in 2023 to USD $4.9 million in 2024. The trend is similar in Latin America where the average cost of a data breach in 2024 amounted to USD $4.2 million, up from USD $3.7 million in 2023. The occurrence of data breaches was widespread, affecting the financial, government, health and telecommunications sectors. These attacks were through DDoS, phishing, ransomware and smishing. More than half of cyber-attacks in Latin America are on Mexico alone (Paleaz-Fernendez, 2024). In 2023, Colombia was hit with a major cyber-attack which led to major disruptions to public and private entities, with indirect impacts on the rest of Latin America (Center for Cybersecurity & Duke University, 2024).

Increased digitization has led to an increase in cyber risk vulnerability which has, in turn, fuelled the introduction of cyber risk laws and committees. The Caribbean was faced with a number of cyber-attacks in the financial and healthcare sector, where attackers gained access to personal and financial data (Caribbean Broadcasting Corporation, 2024; Joseph, 2022; Loop News, 2024; Antigua News Room, 2023). Due to the increase in cyber-crime, Caribbean governments developed initiatives to spread cyber awareness, including specialised units to handle and mitigate attacks. Countries that have enhanced or introduced cyber security strategies include: Barbados, Trinidad and Tobago, Jamaica, The Bahamas, Haiti and Guyana with emphasis on fighting cyber-crime and strengthening cyber security. In 2023, and amended in 2024, Barbados introduced their Cyber Crime Bill, replacing their Computer Misuse Act established in 2003. If found guilty of such, penalties of $100,000 or imprisonment of 10 years serve as punishment. Thus far however, only Jamaica and St. Kitts & Nevis have reported arrests for cyber-crime.

Financial regulation in the Caribbean has also evolved, with cyber risk guidelines and cyber incident reporting forms from the Central Bank of Barbados, Financial Services Commission, and the Central Bank of Trinidad and Tobago. The 2023 Cyber Risk Survey Report indicated that Barbadian banks have developed board-approved cyber security strategies, cyber risk policies, and cyber incident response plans (Central Bank of Barbados; Financial Services Commission, 2024). Spam & phishing was highlighted as the most prevalent cyberattack. Cyber security task forces were also established across the region to respond to breaches. Caribbean governments have also formed partnerships to introduce cyber security programs that focus on bolstering citizens knowledge and capabilities in mitigating and responding to cyber threats. This is a key factor to boost the region's cyber resilience as it helps narrow the gap of the high demand for cyber security professionals worldwide.

Although the Caribbean has strengthened cybersecurity frameworks, there is still room for improvement. The Global Cybersecurity Index identifies the advancements in legal measures as a relative strength of Latin American and the Caribbean. However, the report also notes areas of potential growth in technical, capacity development, cooperation and organisational measures.

Related Work

Defining Cyber Risk

Cyber risk is a significant threat to financial stability. In light of this, it is crucial for financial institutions, especially significant players, to enhance their cyber resilience (Basel Committee on Banking Supervision, 2021). The Financial Stability Board (2018) defines cyber risk as "the probability of cyber incidents occurring and their impact", aligning with the traditional concept of risk. In risk management, consideration must be given to both the likelihood of occurrence and the potential loss. In the context of growing digital financial services and increased prevalence of artificial intelligence, both aspects of cyber risk are intensifying. Artificial intelligence is highlighted as a double-edged sword for cyber resilience as, while it can be used to flag cyber incidents, it is also a key ingredient for the crafting of even more sophisticated attacks (Crisanto, Leuterio, Prenio, & Yong, 2024).

Cyber risk is largely identified as an operational risk to banks in the literature, consistent with Basel guidelines. Cebula and Young (2010) adopt this perspective, defining cyber risk as "operational risks to information and technology assets that have consequences affecting the confidentiality, availability or integrity of information or information systems". This definition highlights the three channels through which cyberattacks can impact financial institutions. Confidentiality refers to unauthorised access to confidential data, availability refers to business disruptions, while the latter refers to the misuse of data. However, Malhotra (2015) critiques this definition as narrow, and places cyber risk in a silo distinct from traditional financial risks. Instead, he contends that cyber risk "subsumes" the traditional financial risk categories as they are often represented by digital information. Expanding on this perspective, Bouveret (2018) notes that cyber risk is not limited to cyberattacks such as phishing, ransomware and denial of service, but can also arise from unrelated events such as software updates and natural disasters.

Cyberattacks can have systemic impacts with that can be widespread, propagating beyond the initially affected institution (Birindelli & Iannuzzi, 2024). This concept is termed systemic cyber risk. Panetta and Leo (2025) define systemic cyber risk as "the potential for a cyber-attack or breach to cause widespread disruption and instability across financial systems and markets". The authors attribute this to the fact that there is widespread use of common information technologies and increased reliance on cloud technologies. This underscores the criticality of gaining a comprehensive understanding of the interconnectedness among financial institutions. The authors also note that reputational risk can result in contagion effects, where customers of unaffected banks lose confidence and reduce their claims on their banks.

Cyber Risk Regulatory Frameworks

While the Basel III framework serves as the international global regulatory framework for managing cyber risk, it is criticised as being inadequate (Peihani, 2022; Krüger & Brauchle, 2021). The criticisms are based on its treatment of cyber risk as operational risk and the calculation approach. Cyber risk is subsumed under operational risk, which overlooks the distinct characteristics of cyber risks such as its systemic characteristics and its exponential nature in terms of type of threats and size of losses.

Doerr, et al. (2022) note the cruciality of quantifying cyber losses for decision-making by regulators regarding cybersecurity investments and the pricing of cybersecurity insurance. This

is difficult given the data constraint relating to cyber incidents and their impacts. The transition from the Advanced Management Approach (AMA) in Basel II to the Standardised Management Approach (SMA) in Basel III also underpins the insufficiency of the Basel II guidelines in calculating required capital for operational risks. The SMA provides a simplified framework but is relatively less risk sensitive than the AMA as it does not account for intra-bank granularity via the various business lines and does not include the use of internal models by the banks. Also, the SMA is backward-looking, based upon 10 years of historical loss experience which may not be useful in estimating potential future cyber risk losses and the necessary capital charges. This downfall is critical given the evolving nature of cyber threats and the fact that underestimation of cyber risk exposures could hinder proactive cybersecurity investments and sufficient provisioning.

Determinants of Cyber Risk Costs and Exposure

Given its systemic nature, cyberattacks are costly to firms and the broader economy. There has been a growing body of literature assessing the drivers of cyber risk and the determinants of cyber risk exposure. Aldasoro et al. (2020) examined the determinants of costs associated with a cyber risk event, utilising a dataset of 155,415 cyber incidents from Advisen[3]. The authors applied a linear regression at a cross-sectional event level, modelling cyber costs as a function of firm size (measured by their revenues), connections (the number of related events) and the intent of the hacker (malicious or not). Results indicated that firm size and connections were positively related to the costs of a cyber event, while malicious intent is negatively correlated. The elasticity of firm size to cyber costs is found to be relatively low at 0.23 to 0.26 percent, but statistically significant. In contrast, Bouveret (2018), found no positive relationship between size and cyber costs. Rather, he found that smaller firms tended to face greater cyber losses. This is plausible as smaller firms often have lower investments in cyber security and resilience measures that leave them more vulnerable to cyberattacks. Unlike firm size, cyber costs are highly sensitive to the number of firms affected, signifying the amplifying role that financial sector interconnectedness plays. Cyber costs increase by 1.8 to 2.2 percent for each additional event connected to the same cyberattack. Interestingly, malicious attacks are correlated with lower cyber costs, measuring up to 60 percent lower (Aldasoro et al., 2020). The authors explain that this may be due to the fact that firms implement significant cyber security measures against such incidents, but cyber losses from other simple errors including human errors are greater. However, further analysis reveals a positive relationship associated with more severe cyber loss events. This suggests that there may be malicious attacks that are seeking large amounts from banks.

Jamilov et al. (2021) expanded on the literature, providing firm-level evidence on the drivers of cyber risk exposure. Cyber risk exposure is measured via text from earnings call, and calculated as the sum of mentions of cyber-related terms divided by the total number of words in the earnings call. Their findings indicate that businesses that hold more assets, have greater liquidity and also have a higher proportion of intangible assets carry greater cyber exposure. For banks, there is still a positive correlation between size and cyber risk exposure. Other significant determinants for banks include their investments in fixed assets and book-to-market equity.

[3] Advisen provides data and technology solutions for the financial sector, particularly the insurance industry. The company's dataset includes data on global cyber incidents.

Cy-VaR: Quantifying Cyber Attack Losses

One of the earliest cyber risk frameworks highlight two values at risk from cyber threats; the assets and reputation of institutions (World Economic Forum; Deloitte, 2012). Assets refer to data, networks and equipment which can all lead to business interruptions under a cyber threat. Reputational damage refers to the erosion of stakeholders' trust and confidence in the organisation which can result in further financial losses through the loss of sales, customers, investments and/or financing. Further work in 2015 resulted in the conceptualisation of Cy-VaR, a quantification framework of cyber risk based upon a value-at-risk model (World Economic Forum; Deloitte, 2015; Orlando, 2021).

This proposed methodology accounts for three (3) components: vulnerability, assets (tangible and intangible), and profile of attacker. The level of vulnerability is determined by an institution's investment in cybersecurity and cyber risk management. This signals the importance of regulators understanding and collecting data on the state of cyber systems, strategies and resilience plans of financial institutions. The European Central Bank has launched a cyber resilience stress test that involves the actual testing of banks' resilience against a fictitious cyber scenario that affects their core database systems. The methodology combined qualitative questionnaires, on-site supervision for IT recovery testing and quantitative data analysis. The survey questionnaire (395 questions) was utilised to capture info on incident reporting cyber policies among other things. While the combined methodology provided great detail for their scenario, it is also difficult to replicate in the absence of appropriate data. Furthermore, the industry's responses could be influenced negatively by such a lengthy survey instrument. As seen by the results of Aldasoro et al. (2020), the profile of attacker is an important as the intent of the attacker is a significant factor in cyber event losses. Assets is the core component of Cy-VaR and is a key input to quantifying the potential losses of a cyber event.

The European Systemic Cyber Group proposed a conceptual model to analyse cyber risk, largely aligning with the asset component from WEF (2015). It comprises four phases including; the context of a cyber incident, the shock that results in the initial immediate impact, the amplification which explores the interconnectedness among firms, and the systemic event which will cause the financial system to fall below a certain threshold (European Systemic Risk Board, 2020).

Bouveret (2018) presents a clear methodology for the quantitative assessment of cyber risk for the financial sector. The methodology follows a VaR type framework, in line with the Cy-Var framework proposed. First, the author models cyber losses using a log-normal distribution for the bulk of losses and then General Pareto Distribution (GPD) for right-tail losses in accordance with the extreme value theory. The losses were obtained from cyberattacks recorded in the ORX News dataset. In the next step, the author models the frequency of cyber events using a Poisson distribution, with an average of 990 events per year as the baseline scenario. In an adverse scenario, the frequency of attacks increases to twice its observed peak. The results indicate that cyberattack losses can amount to 9 percent of banks net income under the baseline scenario and increase dramatically to 26 percent of net income under the adverse scenario. Factoring in contagion effects, with a 20 percent probability that each attack affects multiple institutions, the resulting losses rise from 9 percent and 26 percent to 12 percent and 34 percent

of net income, respectively. The results underscore the amplifying role of interconnectedness in cyber risk propagation. These results concur with the positive relationship between related cyber costs and related events found by Aldasoro et al. (2020). Additionally, Bouveret (2018) notes that this VaR methodology is sensitive to the choice of probability distributions for losses and incomplete data. Monte Carlo simulations are used to estimate the probability distribution of aggregate losses, measured as the product of losses and the frequency of cyber events per year.

In modelling the frequency of cyberattacks, the literature commonly applies two discrete probability distributions; the Poisson and Negative Binomial distributions. While Bouveret (2018) employs a Poisson distribution, several studies argue that the Negative Binomial distribution better captures the overdispersion of cyber events observed in large datasets (Bakdash, et al., 2018; Edwards, Hofmeyr, & Forrest, 2016; Leslie, Harang, Knachel, & Kott, 2018). This finding holds irrespective of the nature of cyber events studied. With a Poisson distribution, however, the mean and variance are assumed to be equal. The Negative Binomial model allows for greater variance than the Poisson distribution, where the mean and variance are assumed to be equal, making it more suitable for capturing the irregular and volatile nature of cyberattacks. Despite this limitation, the Poisson distribution remains useful due to its simplicity, ease of interpretation, and suitability for modelling the frequency of rare and independent events over a fixed time period. Furthermore, the fact that it requires a single parameter is a key advantage in a data-scarce context.

Another group of studies focus on how cyberattacks disrupt financial systems, particularly payment systems. Kotidis and Schreft (2022), through natural experiment, examine the impact of a multi-day cyberattack on Fedwire. The authors used confidential daily payments data to analyse the impacts of such an attack. Results from a difference-in-differences model reveal that users of the system sent 15 percent fewer payments than non-users, with the most significant impact on the first day. On the first day users' transactions were 50 percent lower. This created significant liquidity constraint, as non-users were unable to receive payments needed to facilitate further transactions. Ultimately, during such time, the role of the monetary authority as a lender of last result becomes critical. While some large banks were able to draw down on excess reserves to meet liquidity needs, smaller banks relied on the discount window. This paper provides a clear outline of the transmission of a cyberattacks on a payments system to system liquidity but given the underreporting of cyberattacks and their impact, their natural experiment methodology cannot be easily replicated.

Similarly, Duffie (2019) analyses propagated cyber runs, where large depositors from unaffected institutions withdraw funds due to reputational concerns. Eisenbach, et al. (2021) employ a threshold-based approach to assess the impact of a cyberattack on a wholesale payments system. Institutions are considered impaired if their end of day reserve requirement is at least two standard deviations below its 30-day average. Their findings reveal that a single-day attack impairs 4.8–8.5 percent of institutions, with aggregate losses reaching 5 percent of risk-weighted assets or 37 percent of Tier 1 capital. In a five-day cyberattack, over 50 percent of the banking sector (by assets) faces significant impairment, demonstrating the severe consequences of prolonged cyber disruptions. The authors' definition of impairment is simple and their analysis allowed them to map out the transmission from the top institutions to others.

Cyber risk is a growing and systemic threat to financial stability, necessitating enhanced measures for monitoring, quantifying potential losses and measuring cyber resilience. The Cy-VaR framework stands as a simple, and highly relevant methodology to apply. Existing literature highlights the amplifying role of the interconnectedness of financial institutions, making it crucial to obtain data and information in that regard. While real-world case studies on cyberattacks affecting payment systems and bank liquidity underscore the urgency of mitigating cyber risks, it is difficult to adopt such methodologies without the appropriate transaction level data. The Cy-VaR quantitative modelling approach is useful for estimating potential losses but results are sensitive to the choice of underlying probability distributions.

Methodology, Data and Scenario

In this paper we apply a Value-at-Risk framework, which addresses the backword-looking and less risk-sensitive nature of the SMA proposed under Basel III guidelines. Loss distributional approaches for operational risk, such as this Cyber-VaR framework is advantageous as they model the frequency and severity of potential losses which provides a forward-looking aspect to capital requirements (Bouveret, 2018). This methodology is also particularly useful given the absence of granular cyber risk data.

Scenario

This paper investigates the potential losses associated with a BIN attack on debit cardholders in Barbados. A BIN attack involves fraudsters exploiting algorithms to obtain valid BIN numbers, the first six to eight digits of a payment card, which identify the card issuer and geographic region, providing essential data for fraudsters to generate valid card numbers. These generated numbers are then used to make unauthorised purchases.

Additionally, we assume that banks are held accountable for refunding customers who incur losses due to fraudulent transactions. As discussed in Section 2, BIN attack losses are typically characterised by small values but high frequency. Thus, we anticipate a right-tailed distribution, with the majority of losses occurring at lower values, and the occurrence of larger fraud losses being relatively rare but impactful.

Estimating Total BIN Attack Loss

The aim of the study is to estimate potential losses from a BIN attack. To do this, we employ the Cy-VaR approach to estimate a probability distribution of potential losses due to a BIN attack. As noted in (World Economic Forum; Deloitte, 2015), this approach is simple and yet effective even with the lack of data as it can be used in conjunction with simulation techniques like Monte Carlo simulations. Still, we acknowledge the caveat that our choice of underlying distributions will impact the results (Bouveret, 2018).

Unlike Bouveret (2018), who used a detailed dataset with information on losses, we do not have access to similar data. Instead, we focus on identifying the key variables influencing annual BIN attack losses. We therefore propose the following:

$$Annual\ BIN\ Attack\ Loss\ = f(C, L, D, A, R) \quad (1)$$

where:

C = Number of compromised cards per day
L = Fraud loss per card per day
D = Number of days to detection
A= Number of BIN attacks per year
R = Card Replacement Cost

Total Annual Loss is then calculated as:

$$Annual\ BIN\ Attack\ Loss\ =\ C \times L \times D \times A \times R \quad (2)$$

Assigning Probability Distributions

- **Number of Compromised Cards per Day (C)**

Frequency distributions are particularly useful for assigning the number of loss events in operational risk modelling (Spislak, 2017). There are other discrete probability distributions. Mainly Poisson or negative binomial used in literature. Negative binomial is based on number of failures preceding a set number of success events. We want to model number of events within a fixed time period so Poisson is better. To model the number of compromised cards per day, we assume a Poisson distribution, reflecting the random nature of cyberattacks. This aligns with existing studies where the frequency of cyberattacks is mainly modelled as a Poisson process (Orlando, 2021). The probability of n cards being affected in a given day is:

$$Pr(C = n)\ =\ \frac{\lambda^n}{n!}e^{-\lambda},\ \text{n = 0, 1, 2, …} \quad (3)$$

such that:

$$E(C) = Var(C) =\ \lambda \quad (4)$$

Given the absence of cyberattack loss data in Barbados, this study approximates λ based on a publicly available case study. In June 2022, Homeland Credit Union in Ohio, USA reported that 7 percent of its members were affected by a BIN attack through a merchant system, with impact spanning 24 hours (Homeland Credit Union, 2022). Although the Homeland Credit Union attack occurred abroad, the scenario is applicable to Barbados as domestic banks have also faced card-based fraud risk through merchant systems (Starcom Network, 2022). In modelling the financial impact of a BIN attack for Barbados, we consider demand and transferable deposit accounts as they provide on-demand access to funds and are typically linked to debit cards. We apply a similar compromised card rate of 7 percent and this amounts to 24,270 cards affected, assuming each account is associated with a unique card. Our estimate is in line with IBM's reported average of 28,200 comprised records per data breach and falls well within IBM's observed range of 2,100 to 113,000 compromised records per breach. Thus, the proportion of affected cards is reasonable, making the case for a plausible scenario.

- **Fraud Loss Per Card Per Day (L)**

Using data from LexisNexis (2016), a global dataset on card fraud, average fraud loss in the USA amounted to USD $2.80 or BDS $5.60 per debit card. After applying the cumulative inflation rate of Barbados, we estimate an average loss per card per day of USD $3.48 (BDS $6.97). Losses are expected to be right-tailed, with a bulk of the distribution located at lower values

but we acknowledge that there be some higher than normal losses, resulting in a right-skewed distribution. As such we fit fraud loss per card per day to a log normal distribution.

The log normal distribution is heavy tailed making it appropriate for fraud loss per card per day. For any random number of L:

$$E(L) = e^{\mu+\frac{\sigma^2}{2}} \quad (5)$$

Given the lack of historical loss data for the Caribbean, we apply a standard deviation of 1.9 from Bouveret (2018). The expected fraud loss per card per day is given by:

$$E(L) = \mu = 0.132 \quad (6)$$

- **Days to Detection (D)**

The authors note that the increasing use of AI in fraud-detection systems can result in real-time detection through appropriate notification requests, and automatic card blocking after observing suspicious card activity (MasterCard, 2024). For this reason, we model days to detection as a constant of 1 for simplicity.

- **Number of Attacks per Year (A)**

Based on public news reports, there was one (1) reported data breach in the financial sector in 2022, an averted security breach in 2023, and two (2) reports of local cyber events in 2024 (on April 17 and October 8). Additionally, data from the University of Maryland's Cyber Events Database (Center for International Security Studies at Maryland, 2024), which includes records up to October 2024, suggests an average of one cyber event per year for non-financial institutions. While these figures are likely an underrepresentation of actual attacks in the financial sector, they indicate a relatively low frequency of cyber events with minimal variance.

Although the literature suggests that the Negative Binomial distribution is better suited to model the frequency of cyber events due to overdispersion, the observed data suggests otherwise. Given the low frequency and the minimal variance in reported cyber events, the authors believe that the Poisson distribution is more appropriate for this scenario. Specifically, we assume that the number of attacks per year will vary randomly, and follow a Poisson distribution with $\lambda=2$, reflecting the observed frequency of cyber events in 2024.

- **Card Replacement Costs (R)**

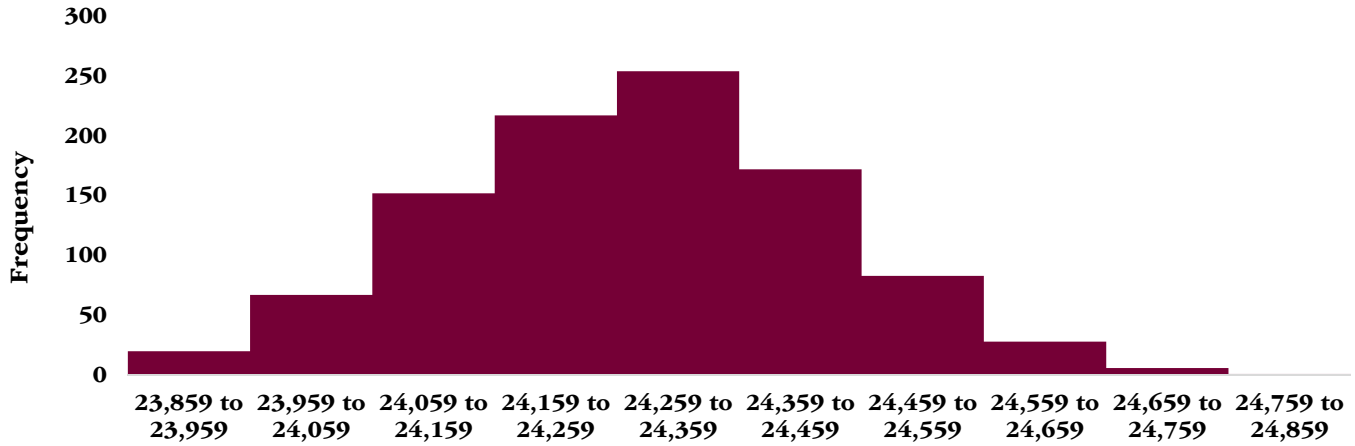
Data obtained from local banks' websites indicate that majority of banks charge USD $10 or BDS $20 for card replacement. Hence, we assume in the case of a BIN attack banks will bear this replacement cost as they replace cards for compromised customers. This value is modelled as constant per card.

Results

We run 1,000 Monte Carlo simulations for each of the key variables in calculating the total BIN attack loss. The simulations were based on the parameters and underlying distributions set in Section 3. The resulting distributions are illustrated below. The number of comprised cards per

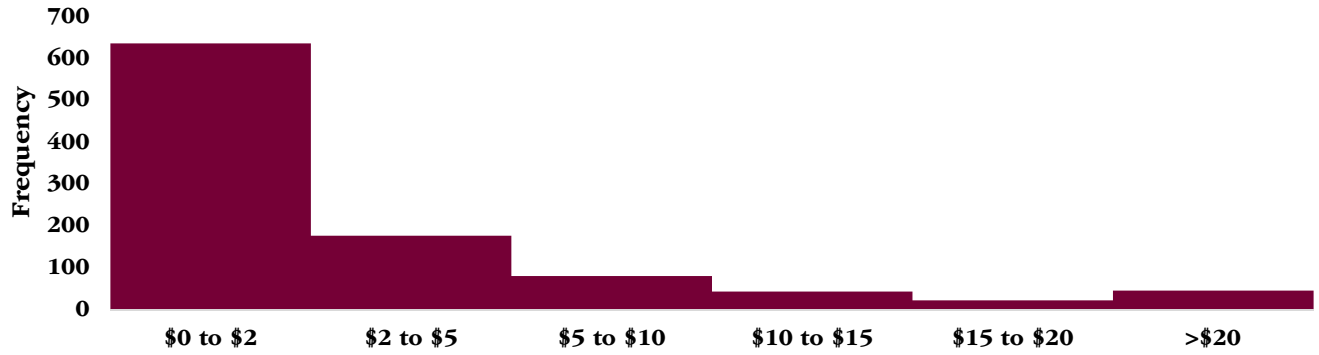
day is within a narrow range of 23,859 to 24,859 cards, inherent to the assumption of equal mean and variance in the Poisson distribution. As expected the distribution of fraud loss per car card is a right-skewed distribution, with a median loss of BDS $5.04 and a maximum of $259.39. The frequency of BIN attacks ranges from none to 10, with an average of 2 BIN attacks per year.

Figure 1: Distribution of Compromised Cards



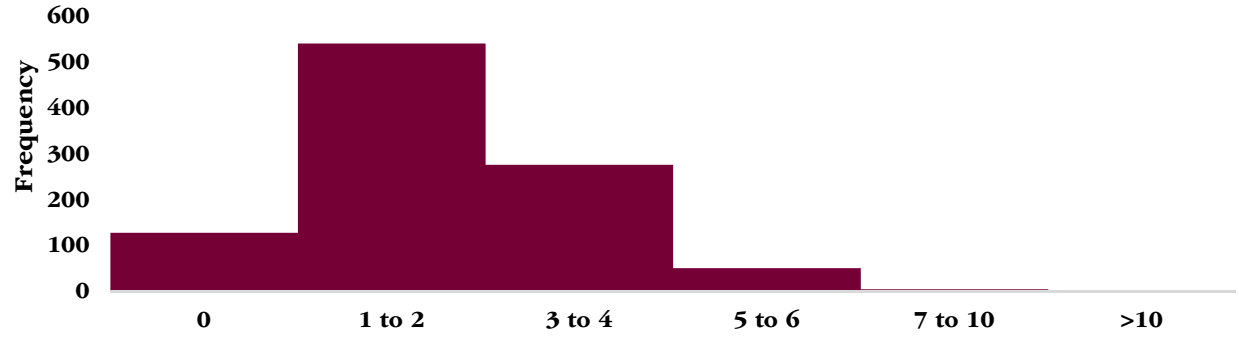
Source: Authors' Calculations

Figure 2: Distribution of Fraud Loss per Card



Source: Authors' Calculations

Figure 3: Distribution of BIN Attacks Per Year



Source: Authors' Calculations

Table 1: Descriptive Statistics of Key Variables

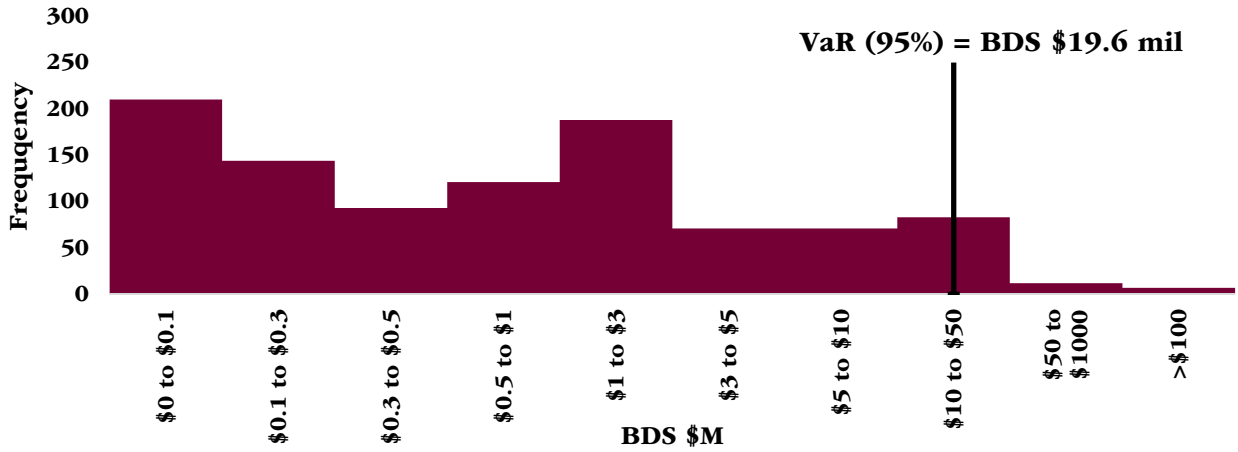
	Number of Compromised Cards	Fraud Loss Per Card Per Day	Frequency of Attacks Per Year
Mean	24,274	5.04	2
Median	24,276	0.99	2
Min	23,859	0.01	0
Max	24,798	258.39	10
Std dev	156	16.22	1

Source: Authors' Calculations

The Cy-Var analysis reveals that banks could lose an average of BDS $5 million each year related to BIN attacks. This is just above half of the global average cost of a data breach (IBM, 2024). This amount represents 2.8 percent of banks' net income and a 1 percent increase in banks operational expenses as at December 2024. Additionally, it is estimated that there is a 5 percent chance that lossess from a BIN attack could exceed BDS $19.6 million (VaR 95 percent). This would cause banks' operational expenses to rise by 3.8 percent and erode 11 percent of their net income. In even more severe cases, the worst 5 percent of cases, expected shortfall could reach up to BDS $60.9 million (ES 95%). The VaR 99% and ES 99% is even larger at BDS $81.2 and BDS $159.1 million, respectively, capturing the worst 1 percent of scenarios. The most extreme possible annual BIN attack loss based on the simulations is estimated at BDS $335.5 million, almost double banks' 2024 net income.

Despite those potential losses, the banking sector remains resilient. Even in the worst case scenario, with the maximum potential loss of $335.5 million, the impact on the sector's capital adequacy is modest. The CAR is reduced by 3.5 percentage points from 21.2 percent as December 2024 to 17.7 percent. Hence, remaining well above the minimum capital requirement.

Figure 4: Distribution of Annual Losses



Source: Authors' Calculations

Table 2: Descriptive Statistics of Potential Annual Losses

Average	$5,033,460.19
25th percentile	$153,268.05
Median	$650,360.94
75th percentile	$2,831,915.50
95th percentile	$19,568,103.68
99th percentile	$81,167,825.52

Source: Authors' Calculations

Table 3: Annual Losses

	BDS $Mil	% of Net Income	% Increase in Operational Expenses	Resulting CAR (%)
Average Potential Loss	5.0	2.8	1.0	21.1
VaR (95%)	19.6	11.0	3.8	21.0
ES (95%)	60.9	34.2	11.7	20.6
VaR (99%)	81.2	45.6	15.6	20.3
ES (99%)	159.1	89.3	30.6	19.5
Maximum Potential Loss	335.5	188.4	64.5	17.7

Source: Authors' Calculations

As noted in the literature, cyberattacks can result in reputational damage which erodes customers' confidence in their banks. To approximate reputational damage, we utilise estimates of cash outflow under daily deposit runs at a rate of 5 percent, the minimum daily deposit run rate utilised in Central Bank of Barbados' liquidity stress test. While it will not have significant liquidity impacts given the highly liquid conditions of the banking sector, cash outflow totals BDS $630 million on day one. This cash outflow is substantially greater than the 95% VaR loss, signalling that reputational loss and other indirect losses can be potentially more substantial than first-round direct losses. Beyond this, we note the possible repercussion on the real economy stemming from interruptions in payments systems which have negative implications for consumption activity.

Conclusion

In this paper, we apply a VaR framework to quantify potential losses from BIN attacks on the Barbadian banking sector. Cy-VaR is a simple yet effective framework for the examination and quantification of cyber risk. Conceptually, it acknowledges that both banks assets and reputation are at risk to cyber threats and provides a comprehensive scope of cyber risk by encompassing the three components of vulnerability, assets and profile of attackers. The first component underscores the need to examine cyber interconnectedness in the financial sector, making the case for detailed cyber resilience stress tests. It is important to consider the profile of the attacker as empirical evidence shows that both malicious intent and simple human errors result in substantial cyber losses. The asset component is at the core of loss quantification. Such estimates are critical for individual financial institutions, to guide their cybersecurity

investments, and for central banks, to assess the ability of the banking sector to withstand cyberattacks.

References

Aldasoro, I., Gambacorta, L., Giudici, P. & Leach, T., 2020. *The Drivers of Cyber Risk,* s.l.: Bank for International Settlements.

Antigua News Room, 2023. *Antigua News Room.* [Online] Available at: https://antiguanewsroom.com/hackers-reportedly-wreak-havoc-on-apuas-billing-system/
[Accessed 27 March 2025].

Bakdash, J. Z. et al., 2018. Malware in the Future? Forecasting of Analyst Detection of Cyber Events. *Journal of Cybersecurity,* pp. 1-10.

Barbados Today, 2020. *Financial institutions move to VISA and MasterCard as CariFS system ends,* Bridgetown: Barbados Today.

Basel Committee on Banking Supervision, 2021. *Principles for Operational Resilience,* s.l.: s.n.

Birindelli, G. & Iannuzzi, A. P., 2024. The Systemic Importance of Cyber Risk in Banks. In: *Systemic Risk and Complex Networks in Modern Financial Systems.* s.l.:Springer, pp. 301-322.

Bouveret, A., 2018. *Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment,* s.l.: s.n.

Caribbean Broadcasting Corporation, 2024. *Caribbean Broadcasting Corporation.* [Online] Available at: https://www.cbc.bb/news/local-news/hackers-breach-barbados-statistical-service-systems/
[Accessed 28 March 2025].

Cebula, J. J. & Young, L. R., 2010. *A Taxonomy of Operational Cyber Security Risks,* s.l.: s.n.

Center for Cybersecurity & Duke University, 2024. *LATAM CISO,* North Carolina: Duke University.

Center for International Security Studies at Maryland, 2024. *Cyber Events Database,* s.l.: University of Maryland.

Central Bank of Barbados; Financial Services Commission, 2024. *Financial Stability Report 2023,* s.l.: s.n.

Crisanto, J. C., Leuterio, C. B., Prenio, J. & Yong, J., 2024. *Regulating AI in the Financial Sector: Recent Developments and Main Challenges,* s.l.: s.n.

Cunningham-Marsh, J., 2024. *The State of OT Cyber Security in Latin America 2024 Annual Report,* s.l.: s.n.

Decisimo, 2024. *The rising threat of BIN attacks: Understanding, adapting, and protecting*. [Online]
Available at: https://decisimo.com/antifraud/bin-attacks.html
[Accessed 16 April 2025].

Doerr, S. G. L. L. T., Legros, B. & Whyte, D., 2022. *Cyber Risk in Central Banking,* s.l.: Bank for International Settlements.

Duffie, D. & Younger, J., 2019. *Cyber Runs,* s.l.: s.n.

Edwards, B., Hofmeyr, S. & Forrest, S., 2016. Hype and Heavy Tails: A Closer Look at Data Breaches. *Journal of Cybersecurity,* pp. 3-14.

Eisenbach, T. M., Kovner, A. & Lee, M. J., 2021. *Cyber Risk and the U.S. Financial System: A Pre-Mortem Analysis,* New York City: Federal Reserve Bank of New York.

European Systemic Risk Board, 2020. *Systemic Cyber Risk,* s.l.: s.n.

Europeran Central Bank, 2024. *ECB concludes cyber resilience stress test,* s.l.: s.n.

Financial Stability Board, 2018. *Cyber Lexicon,* s.l.: s.n.

Franklin, J., Paxson, V., Perrig, A. & Savage, S., 2007. *An Inquiry into the Nature and Causes of the Wealth of Internet Miscreants*. s.l., s.n., pp. 375-388.

Healey, J., Mosser, P., Rosen, K. & Tache, A., 2018. *The Future of Financial Stability and Cyber Risk,* Colombia: The Brookings Institution.

Homeland Credit Union, 2022. *Blog: Important Notice: Debit Card Fraud*. [Online] Available at: https://www.homelandcu.com/about-us/blog/blog/2022/06/06/important-notice-debit-card-fraud

IBM, 2024. *Cost of a Data Breach,* s.l.: s.n.

IMF, 2024. *Global Financial Stability Report,* Washington: s.n.

ITU, 2024. *Global Cyber Security Index,* Switzerland: Internation Telecommunications Union.

Jamilov, R., Rey, H. & Tahoun, A., 2021. *The Anatomy of Cyber Risk,* s.l.: s.n.

Joseph, E., 2022. *Barbados Today*. [Online] Available at: https://barbadostoday.bb/2022/12/15/qeh-services-impacted-by-cybersecurity-incident/
[Accessed 27 March 2025].

Krüger, P. S. & Brauchle, J.-P., 2021. *The European Union, Cybersecurity, and the Financial Sector: A Primer,* Washington, DC.: Carnegie Endowment for International Peace.

Leslie, N. O., Harang, R. E., Knachel, L. P. & Kott, A., 2018. Statistical Models for the Number of Successful Cyber Intrusions. *The Journal of Defense Modeling and Simulation,* 15(1), pp. 49-63.

Loop News, 2024. *Loop News.* [Online]
Available at: https://www.loopnews.com/content/police-probe-cyber-attack-on-western-union-branch-in-castries/
[Accessed 23 March 2025].

Malhotra, Y., 2015. *Stress Testing for Cyber Risks: Cyber Risk Insurance Modeling beyond Value-at-Risk (VaR): Risk, Uncertainty, and, Profit for the Cyber Era,* New York: s.n.

MasterCard, 2017. *2 Series Bank Identification Numbers,* s.l.: s.n.

MasterCard, 2024. *Mastercard accelerates card fraud detection with generative AI technology.* [Online]
Available at: https://www.mastercard.com/news/press/2024/may/mastercard-accelerates-card-fraud-detection-with-generative-ai-technology/
[Accessed 17 April 2025].

Miles, K., 2025. *Jamaica Observer.* [Online]
Available at: https://www.jamaicaobserver.com/2025/03/28/cyberattacks-climbing-across-caribbean/
[Accessed 29 March 2025].

Orlando, A., 2021. Cyber Risk Quantification: Investigating the Role of Cyber Value at Risk. *Risks,* 9(184), pp. 1-12.

Paleaz-Fernendez, A., 2024. *Mexico faces over half of Latin American cybercrimes due largely to US ties.* [Online]
Available at: https://www.reuters.com/world/americas/mexico-faces-over-half-latin-american-cybercrimes-due-largely-us-ties-2024-10-09/

Panetta, I. C. & Leo, S., 2025. Systemic Cyber Risk in the Financial Sector: Can Network Analysis Assist in Identifying Vulnerabilities and Improving Resilience?. In: *Systemic Risk and Complex Networks in Modern Financial Systems.* s.l.:s.n., pp. 133-153.

Peihani, M., 2022. Regulation of Cyber Risk in the Banking System: A Canadian Case Study. *Journal of Financial Regulation,* 8(2), pp. 139-161.

Satrcom Network, 2022. *Credit/Debit Card Breach update.* [Online]
Available at: https://starcomnetwork.net/blog/2022/05/05/credit-debit-card-breach-update/

Schreft, S. L. & Kotidis, A., 2022. *Cyberattcks and Financial Stability: Evidence from a Natural Experiment,* Washington, D.C.: Federal Reserve Board.

Spislak, M., 2017. *Assessment of Cyber Risk in the Banking Industry,* s.l.: s.n.

Starcom Network, 2023. *Starcom Network.* [Online]
Available at: https://starcomnetwork.net/blog/2023/02/22/cob-cyber-attack/
[Accessed 28 March 2025].

The Barbados Parliament, 2024. *Cyber Crime bill.* [Online] Available at: https://www.barbadosparliament.com/bills/details/741

ToolCase, 2022. *Debit Card Holders Victimized by BIN Attack.* [Online] Available at: https://news.toolcase.com/2022/06/13/debit-card-holders-victimized-by-bin-attack/?utm_source=chatgpt.com
[Accessed 16 April 2025].

Trinidad & Tobago News Day, 2023. *News Day.* [Online] Available at: https://newsday.co.tt/2023/02/09/caribbean-faced-144-million-cyberattack-attempts-in-6-months/
[Accessed 28 March 2025].

Visa, 2022. *8-Digit BIN Industry Change,* s.l.: s.n.

White, A. et al., 2024. *The global IT outage: As it happened,* s.l.: s.n.

World Economic Forum; Deloitte, 2012. *Risk and Responsibility in a Hyperconnected World: Pathways to Global Cyber Resilience,* s.l.: s.n.

World Economic Forum; Deloitte, 2015. *Partnering for Cyber Resilience Towards the Quantification of Cyber Threats,* s.l.: s.n.


background
background
}
.box{
position:
top: 50%;
left: 50%;