Journal of Computer Science and Information Technology
June 2018, Vol. 6, No. 1, pp. 1-9
ISSN: 2334-2366 (Print), 2334-2374 (Online)

Published by American Research Institute for Policy Development
DOI: 10.15640/jcsit.v6n1a1
URL: https://doi.org/10.15640/jcsit.v6n1a1

Establishing a Corporate Algorithm to Mitigate Data and Information Privacy Breaches

K. M. Moorning[1]

Abstract

During the last five years, more than nine billion customer records have been compromised. As digital transactions assume greater influence in the day-to-day lives of people around the world, many people want ways to hold businesses accountable for information control. Data breaches are linked to weak internal security procedures and practices, likely due to misconfigured digital systems. Transporting customers' private information online or in global networks to third parties means an increased risk of an outsider gaining deep visibility into confidential information. It is challenging to obtain relief through legislation, and consumers must determine with their own volition which businesses to trust. The fiduciary duty of protecting consumers' valuable information is dissolute, while the secondary market of selling data pulled from businesssystems is rampant.Critical risk perception measures to reduce the severity and vulnerability levels of information misuse should assuage breaches by placing a hefty burden on data protection and control. This research discusses the surge in digital transactions, recent data breaches, e-commerce legislation, and presents a corporate analysis of risk probability (CARP) score as a new measure for analyzing data breach risks.

Keyword: Information Security, Data Breach, Digital Transaction, CARP Scores

1. Introduction

The accelerated use of information and communication technologies for e-commerce and m-commerce by digital buyers indicate that the majority of consumers have grown comfortable with online shopping. In this interconnected economy, electronic relationships exist between consumers and corporations. Businesses engage in e-commerce to offer products and services to a global audience, expand their market base, and strengthen their competitive position. Ingenious methods for investing trust in otherwise anonymous online transactions influence consumers in unprecedented ways to conduct business using digital devices. With minimal effort, these same technologies can shockingly provide the arsenal for an online identity thief to strike. Weak safeguards can cause emotional distress and monetary damage when personal information is lost or stolen. At issue is the risk involved when conducting digital transactions within the confines of the current liability efforts, or whether more effective federal liability standards are required to mitigate privacy harms.

1.1 Rights to Privacy

Privacy is an individual's interest in protecting his or her personal information and the corresponding obligation of entities accessing, using, or disclosing that information to respect those interests through fair information practices. Security means protecting information and an information system from unauthorized access, use, disclosure, disruption, modification, or destruction to guard against improper information modification or destruction and includes ensuring information nonrepudiation and authenticity. Confidentiality means authorizing restrictions on access and disclosure, including means for protecting personal privacy and proprietary information (Fox, 2009).

[1] Department of Computer Information Systems, Medgar Evers College of The City University of New York, Brooklyn, NY 11225, USA. kimm@mec.cuny.edu

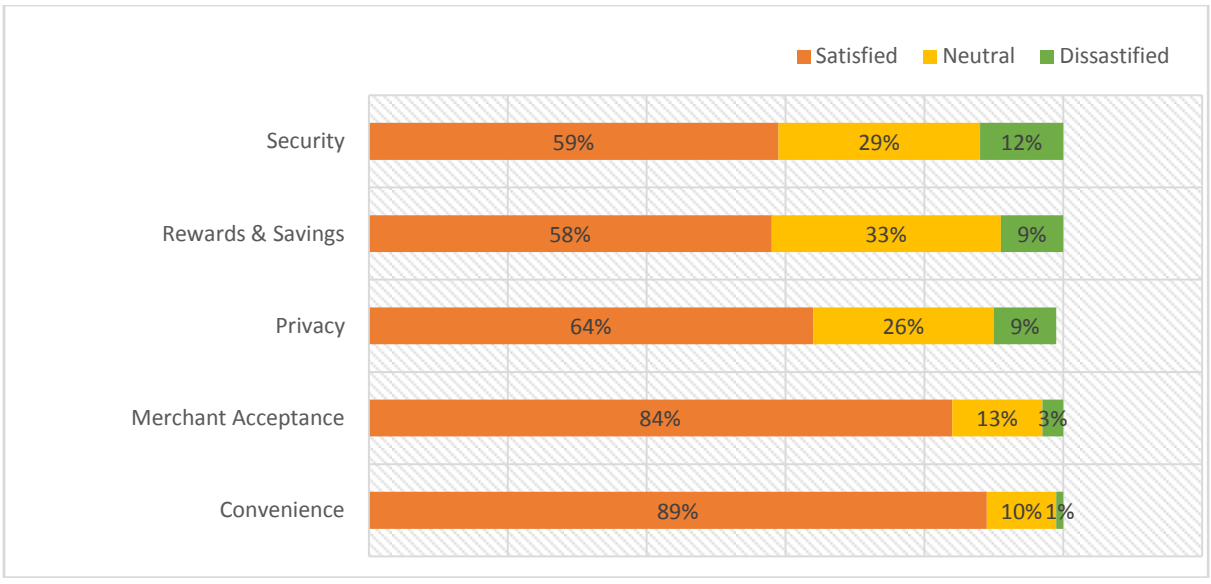
It is argued that because consumers are vulnerable in their dealings with corporations due to information and control deficits, businesses have a moral duty to take reasonable precautions with consumer data and to avoid harm in using this data (Culnan & Williams, 2009).

Corporations sharing information on the Internet need to provide customers with risk factors and recovery efforts. Privacy policies speak to how information is shared or kept confidential but does not address mitigation of information abuse and unauthorized access. Critical risk perception measures determine the severity and vulnerability levels of information misuse to project the amount of hardship a consumer would experience as a result of information leakage. The sharing of proprietary information online requires a sophisticated expectation in business transactions (Moorning, 2013). Throughout the world, the prevalence of data breaches and identity theft has caused major concern about digital transactions. Customers should not only be able to trust that their money and data will be secure but know the degree to which risk reduction efforts are made to prevent harm.

1.2 Digital Transactions

Digital transactions are direct transfers of funds using electronic money in the form of stored values or on-demand payments. From the perspective of a consumer, a payment system provides convenient ways to transfer funds to a person or seller. Payment methods include debit, credit and prepaid cards as well as intermediates such as Apple Pay, Samsung Pay, PayPal, and Mobile Money or digital cash innovations such as Bitcoin and Blockchain. Digital assets include demographics (name, age, date of birth, address, phone, social security number, a photographic image), professional information (employer, salary, resume) and financial information (credit card number, debit card number, digital cash) and all personal information which must be safeguarded. From the perspective of the financial institution, a payment system is a set of procedures and devices that circulate of money. Transfers can be initiated using computing devices, telephones or in stores. Digital payment media includes E-commerce, M-commerce, online banking, automatic teller machines, telephones, e-z pass tolls, and point of sale systems. Findings from a "2015 Consumer Payment" survey indicate that "overall customer satisfaction with digital payments is mixed." Customers "appreciate the fact that merchants accept multiple payment solutions," but see "considerable room for improvement in areas such as privacy, rewards and savings, and security" (Flamme & Greave, 2015).

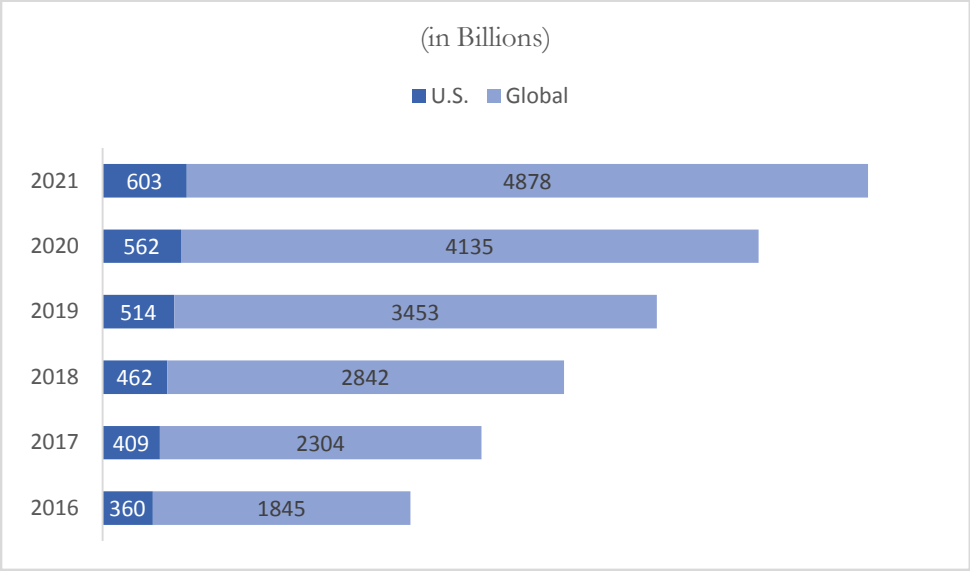
Chart 1 – Consumer Satisfaction with Online & Mobile Payment Solutions



Source: Strategy& - 2015 Consumer Payments Survey

At relatively low overhead, 21-40% of a business's contributions are a direct result of e-commerce transactions and is expected to grow rapidly over the coming years. In the United States alone, online sales of physical goods amounted to $360.3 billion and are projected to surpass $600 billion by 2021.Global retail e-commerce sales are expected to reach $4.8 trillion by 2021.

Chart 2 – Retail E-Commerce Sales from 2016-2021



Source: (Statistica, , 2017)

1.3 Cashless Society

Although people use money on a daily basis for the purchase of goods and services, cash is used less often due to the acceleration of contactless cards and smartphone technology. With the proliferation of e-commerce, mobile devices, and security enhancements, digital payments are certain to increase and likely surpass traditional payment methods in the next few years (Whitehead, 2017). From an ethical standpoint, the argument in favor of e-commerce is straightforward: the public has a vital stake in the outcomes, and therefore it has a right to convenience in commerce. It is questionable whether a fully cashless society would an advance the economy without addressing the privacy and security problems that plague digital transactions. The critical element of e-commerce as a 21st century transaction processing method lies in whether consumers can make meaningful choices about whom they do business with when they have complete information about privacy and controls (Leape, 2010).

2. United States Legislation

The Uniform Electronic Transactions Act (UETA) removes barriers to e-commerce by establishing that electronic records in digital transactions are legally equivalent to manually-signed paper documents. The Payment Card Industry Data Security Standard (PCI DSS) sets requirements forstoring, processing and transmitting customer's credit card data. PCI compliance requires the use of the latest security and authentication techniques, a firewall between the business network and cardholder devices, and a network intrusion detection system. The Fair Isaac Corporation, popularly known as FICO, keeps close tabs on credit files and uses a secret formula to reduce that information to a number that can powerfully impact lives. The Federal Information Processing Standard 199 and the 2002 Federal Information Security Management Act sets levels of information security according to a range of risk levels. Government legislation is associated with consumer feelings of efficacy and empowerment (Parramore, 2011), but the lack of consensus about individual principles creates dissonance between the operationalization and implementation of fair information privacy practices.

Other regulations provided in the Computer Fraud and Abuse Act, Electronic Communications Protection Act, The Stored Communications Act, The Health Insurance Portability and Accountability Act set standards for compliance but not standards for ethics. PricewaterhouseCoopers developed an opacity index that measures the economic effects of risks associated with lack of trust and transparency. According to this model, countries where investors fear dishonesty, corruption, arbitrary administration of laws and policies, lack of standard accounting practices, and other uncertainties pay a measurable economic penalty that affects the ability of their markets to attract investment(Rasmus, 2006).It is important to note that the justification of compliance does not always necessarily have to be normative.

Although there are laws and jurisprudence that manifestly establish a duty to protect consumer information, there are also very basic and practical reasons to convince business leaders of the importance of promoting security, privacy and confidentiality.

2.1 FICO Scores Regulations

As digital transactions exploded, credit bureaus got quite savvy and efficient about rapidly electronically sending out information about consumers. FICO began selling its credit scoring system. The Fair Credit Reporting Act gave consumers the right to view and dispute reports, but not the right to restrict access to their information collected by companies. From an information technology perspective, businesses see investments in compliance as costs with few benefits and no return on investment. The lowest-cost solution is deployed to meets current legal requirements. Lenders want to know something about virtual clients besides their creditworthiness, giving rise to the collecting personal details about customers from other sources. The defense against identity theft and consumer information misuse places the victim at the helm. The credit-scoring business is rife with problems and abuses as millions of Americans watch their credit scores plummet since the financial crash.

3. Information Sharing &Misuse

Culnan & Williams (2009) indicates that while there is a consensus in principle that fair information practices constitute socially responsible information practices, there is no consensus about how the principles should be implemented. In the U.S. there are no comprehensive laws requiring all businesses to observe fair information practices. Both the operationalization and implementation of the fair information practices in the U.S. is uneven. Unfortunately, corporate reforms related to transparency and access to information, however, has received scant attention (Herrero & Lopez, 2010). Much research about information privacy focus on the need for transparency between businesses and stakeholders, and less about privatizing, securing and the confidentiality of consumer information. Leakages have always been a concern for information systems, whether it is through internal espionage, employee sabotage, or plain old ignorance, it is a serious matter when confidential, sensitive, or customer information leaves the network (Rasmus, 2006). The digital paradigm requires a more secure infrastructure for the protection of consumer data and the implementation of policy reforms. Businesses are only obligated to protect the information it generates during its daily operation and customers right to privacy.

3.1 Identity Theft

Identity theft, a major problem in the U.S., was the number one reported consumer complaint with the Federal Trade Commission (FTC) for 15 consecutive years in 2014. During 2015, it launched the IdentityTheft.gov website to help consumers get a personal recovery plan causing identify theft complaints to drop to number two. Table 1 lists the top ten countries for fraud complaints by country of origin.

Table 1 – Top Ten Countries for Fraud Complaints[1]

Rank	Country	Complaints	Percentages
1	United States	1,108,331	96%
2	Canada	17,124	1%
3	United Kingdom	7,591	1%
4	Nigeria	7,501	1%
5	India	7,451	1%
6	Jamaica	6,546	1%
7	China	5,451	<1%
8	Mexico	4,299	<1%
9	Dominican Republic	3,444	<1%
10	Ghana	2,439	<1%

1Percentages are based on the number of fraud complaints received by the FTC between January 1 and December 31, 2015

Several factors can undermine customers' and regulators' confidence in digital transactions. Criminals seek personal gain by attacking databases, and their insidious actions should motivate businesses to adopt strong information security approaches.

The need for protection against cyber-crime, denial-of-service attacks, web hackers, data breaches, identity and credit card theft, and fraud was long identified (Smith, Winchester, Bunker, & Jamieson, 2010). A security breach can lead to loss of customer trust that might last years.

The sharing of information on the Internet and in electronic processing systems has made it easier for a criminalto acquire customer information fraudulently. In 2015, more than 707.5 million data records were compromised down from 1.02 billion records lost or stolen in 2014 (Enterprise Security, 2016).

Table 2 - Data Loss/Stolen by Industry (2015)

Percent	Industry	# of Records
43%	Government	307,122,342
19%	Healthcare	134,385,415
17%	Other	121,129,222
12%	Technology	84,394,833
6%	Retail	40,075,707
3%	Education	19,328,253
<1%	Financial Institution	1,074,043

Source: Enterprise Security

One year later, in 2016, the latest FTC annual list of top consumer complaints report shows that identity theft had dropped to third place, behind debt collection and impostor scams. Table 3 lists the identity theft victim information misuse by types of fraudulent transactions. For criminals who engage in identity theft, the most common type of misuse is to defraud the government (Federal Trade Commission, 2016).

Table 3 – Identity Theft Victim Information Misuse

Type of fraud[1]	Percent
Government (Tax, Wage-Related, Driver's License& Benefits)	49.2
Other Identity Theft Purpose	16.0
Credit Card	15.8
Phone or Utilities	13.1
Phone & Utilities	9.9
Bank fraud	5.9
Attempted Identity Theft	3.7
Loan	3.5
Employment Related	3.3
Other	19.2

*2016 percentages exceed 100% due to multiple types of misuse.

Source: FTC

Changes in retail practices escalate information privacy accountability and force greater responsibility for unexpected leakages. Conflicts with customer priorities or other information values will cause them to seek alternate means of redress increasingly. Transporting customer information online or in global networks to third parties means that outsiders have deep visibility into the private information collected by the organization. The power of technology is a double-edged sword. In some cases, sharing of information digitally is required because increases efficiency, but the haphazard way in which the information is reported and protected leads to increased information abuse. The secondary market of selling consumer information pulled from weak systems is prevalent (Moorning, 2013).

Merchants, issuers, acquirers, processors and service providers have for years recognized the need to take a collaborative approach when tackling online fraud. Juniper's 2017 "Online Payment Fraud" report research provided "a comprehensive analysis of how the landscape is developing, both in terms of fraudster approaches as well as service provider strategies." They examined key industry sectors including: "digital banking, remote physical goods purchases, remote digital goods purchases, digital money transfer, and air ticketing." For these industries, the existing legislation seems to foster a 'pass-the-parcel' approach where one party legitimately passes liability to another. If the digital payment industry is to disrupt fraud seriously, then it is vital that each party take a committed shared approach to combating fraud(Sorrell, 2017).

4. Data Breaches

Hacking is unauthorized access to exploit a computer system or network and take control for some illicit purpose. Data breaches are the compromising of records and information via internal methods or employees. When breaches occur, they expose both the company and the consumer to a great deal of risk and damage. As more business is conducted digitally, and as criminals realize the value of the data being transmitted, society is seeing more big-name, high-profile breaches. Experian, one-third of the giant credit reporting trilogy explains that even though companies are better prepared to protect against a data breach, "attackers are finding more stealthy ways to get around security measures and seek the information they want." Experience of the past decade has shown that even the mature capital markets are not immune from information breaches. Each case of corporate financial misfeasance, whether due to fraud or honest error, diminishes systemic trust, increases risk and creates a more urgent requirement to protect shareholders, the public and the integrity of the markets (Experian, 2017).

Notable data breaches like the Equifax loss of over 143 million records for account holders and Facebook sharing of 50 million Facebook users' private data with United Kingdom firm Cambridge Analytica without their knowledge are those discussed by the media because of the big name involved. However, more than forty data breaches went undisclosed by major corporations in the year 2017 alone. Only 4% of breaches were secure where encryption was used, and the stolen data was rendered useless. Data records are lost or stolen at the current rate of 5,083,804 every day, 211,825 every hour, 3,530 every minute, and 59 every second (Germalto, 2017) yet only 2% IT professionals feel third-party secure access is a top priority (Soha Systems, 2016). Table 4 lists the notable data breaches and the impact it had on up to billions of records (Larson, 2017). Data losses have a lasting impact for years to come and raise specific concerns about the amount of information data brokers collect on consumers.

Table 4 - Notable Data Breaches

Company	Impact (in millions)
Equifax	143
Adult Friend Finder	412.2
Blue Cross Blue Shield / Anthem	78.8
eBay	145
JP Morgan Chase	76
Home Depot	56
Yahoo	3,000
Target	110
Adobe	38

Source:CNN Tech

5. Risk Analysis

In the digital (technology) context, the negative impact caused by malicious information technology (IT) is associated with two dimensions: computer performance and information privacy which are the stimulus that can avoid the threats. Avoidance behavior can enlarge the discrepancy between the risk of breached data leading to a sense of urgency that motivates customers to take their own safeguarding measures (Liang & Xue, 2009).Risk reduction behaviors are necessary to protect consumers even in the absence of legislative mandates. All digital transactions carry some risk, but some are much riskier than others. Risk is the subjective judgment people make about the severity and probability of risk.

It is the medium between the impossibility and the possibility of an occurrence of a specified event. Risk analysis is divided into two components: 1) risk assessment – identifying and evaluating the probability and severity of risks, and 2) risk management - deciding proper intervention behaviors to mitigate risks and what to do about when events occur.

5.1 Probability Risk Analysis (PRA)

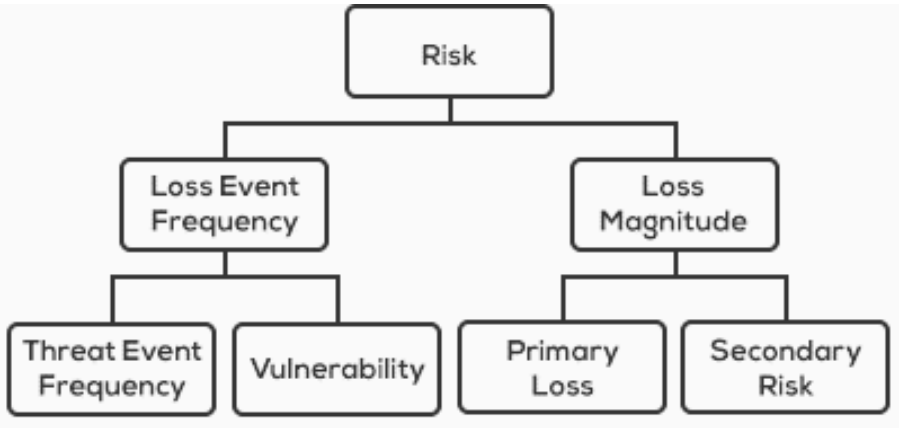
Risk analysis estimates risk based on the event and threats to that event (also called hazard). Estimates range from moderate to severe to catastrophic based on a calculated probability over the possible consequence. Also referred to as probabilistic risk analysis (PRA), this estimate seeks to describe the consequences in terms money, time, or data loss.

PRA often seeks to determine 1) what can happen, 2) how likely it will happen, and 3) what are the consequences. In PRA, risk (R) is a set of triplets, R={<si,pi,ci>}, where "i" is an incident, "si" is scenario i, pi is the probability of scenario i, and ci are the consequences if scenario i occurs. N would represent the total number of scenarios. PRA is increasing in importance for analyzing the risks of digital adversaries who seek to harm a system or people.

5.2 Factor Analysis of Information Risk (FAIR)

The "Factor Analysis of Information Risk" (FAIR) method developed by Jack A. Jones is devoted to the analysis of different factors influencing the information technology (IT) risk. A factor is anything that influences the frequency or impact of a risk scenario. It can be a lost card by a client or an exploited company database.Risks reflects the causal factors of a scenario materializing based on expected or pre-disposed threats. Risk management evaluates threats in digital systems to determine whether they are faulty (bad design, accidental, ineffective execution) or malicious (inappropriate use, theft). The timing, detection, and reaction of the data loss are critical in estimating the loss magnitude and negative impacts. The scenario and the threat are two components of risk *(R) that are used to determine* potential loss *(L)*, and probability *(p)* that the loss will occur. Acceptable risk is an understanding that some scenarios are tolerated because the cost or difficulty of implementing an effective countermeasure exceeds the expectation of loss(The Open Group, 2014).

Chart 2 - Factor Analysis of Information Risk



Source: FAIR Institute

5.3 Quantitative Risk Assessment (QRA)

Quantitative Risk Assessment (QRA) assigns a dollar value to risk for each single loss expectancy (SLE), then multiplies this value by the annual rate of occurrence (ARO). For example, if the value of the loss is $500 and the ARO is 10, then for an SLE ($500) times the ARO (10), the event loss is $5,000. However, other costs such as those to control the event, protect the system from future events, train staff, and unexpected client loss will also affect the dollar amount in the total loss. This research proposes conducting risk analysis from a legislative perspective. It advances the principles of QRA, PRA, and FAIR to produce scores that assess the probability of risk for a given organization. FICO (Fair Isaac Corporation) created the score used to measure consumer credit risk in the U.S. by the three major credit reporting agencies Equifax, Experian, and Transunion. A similar risk algorithm can produce a credit risk score for organizations that engage customers in digital transaction or e-commerce.

5.4 Corporate Analysis of Risk Probability (CARP)

Since breaches have varying degrees of fallout ranging from compromising entire global networks to others having little to no impact whatsoever, a breach level index (BLI) is needed to track publicly disclosed breaches. Organizations are still required to do their own risk assessment based on a few simple inputs that will calculate their risk score, overall breach severity level, and summarize actions IT can take to reduce the risk score(Gemalto, 2017).A corporate analysis of risk probability (CARP) score would quantify the businesses' BLI, frequency of data breaches, amount of loss, risk management plan, length in time in business, and frequency of digital transaction to determine their public digital transaction risk for all companies regardless of whether they've experienced a data breach.A distinction is made between the impact weight of each of the areas in this mathematical construct.

The history of data breaches would differ for a newly formed corporation than for a corporation which has been in business for a lengthy period. In the same way, the number of digital transactions for a company without a data breach would positively increase the score. The size of the corporation is a mitigating factor since smaller companies have less internal controls over their client data. The higher the CARP score, the less risky it is in conducting a digital transaction with the corporation. Table 5 compares the risk factors and weights for FICO scores to the proposed CARP score.

Table 5 – FICO vs CARP

COMPARISON OF FICO SCORE WITH CARP SCORE			
FICO Factor	**FICO Weight**	**Proposed CARP Factor**	**Proposed CARP Weight**
Payment history: Account payment information, delinquencies and public records.	**35%**	**History of data breach** Measures the frequencies of data breach over time	**35%**
Amounts owed: How much is owed on accounts. The amount of available credit on revolving accounts.	**30%**	**Amount of loss from data breaches** Calculates the total loss to clients and to the business per event.	**30%**
Length of credit history: How long accountsis open and time since last account activity.	**15 %**	**Types of risk management plans** Measures the extent the business can compensate clients' losses and recover.	**15%**
Types of credit used: The mix of accounts (e.g. revolving & installment.	**10%**	**Length of time in business** Measures the professional position	**10%**
New credit: Pursuit of new credit, credit inquiries and number of recently opened accounts.	**10%**	**Number of transactions** Measures customer loyalty and trust	**10%**

6. Conclusion

Business policies and government e-commerce legislation establish acceptable levels of risk, but the level of risk is cloudy for consumers. Risk management plans must ensure that when systems are set up to process digital transactions, the required actions to manage the assessed risks are in place. These procedures should be made available to the public to provide feedback on the effectiveness of both the planned procedures and decisions made in response to data breaches. Consumers hold the greatestresponsibility for protecting their digital assets, i.e., their personal information stored in digital form. Data points collected on paper forms and computer-based forms creates a relationship between customer and the business. Trusting an organization to manage any of a customer's information is a privilege that businesses must hold sacred. On the other hand, customers have the option of locking credit reports, government records, and requiring bank alerts when a digital transaction occurs. Thismitigates access and reduces the response time in data breach events.

This CARP approach to risk management will have implications for legislation across the digital transactions value chain. Each company should think through and understand its own risk and use that guidance for conducting business. The transparency of data controls that protect consumer information mitigates the potential adverse consequences of each data breach. Developing contingency plans and continuity procedures for managing risk efficiently are some ways to build consumer trust, but business need transaction insurance, in the form of capital and liquidity reserves allocated for potential losses. Such reserves should equal the amount of financial impact if all clients were affected.

The U.S has legislation requiring business and governmental entities to notify individuals of security breaches of information involving proprietary information. The notice of a breach is inadequate to combat the losses consumers experience as a result of personal information mismanagement. Legislators and regulators need to assess whether transaction insurance makes digital accounts as safe as regular deposits.

Bibliography

Culnan, M. J., & Williams, C. C. (2009, December). How Ethics can Enhance Organizational Privacy: Lessons from the Choicepoint and TJX Data Breaches. MIS Quarterly, 33(4), pp. 673-687.

Enterprise Security. (2016). 2015 Data Breach Statistics: The Good, the Bad and the Ugly. Gemalto: Enterprise Security.

Experian. (2017). Data Breach Industry Forecast. Costa Mesa: Experian.

Federal Trade Commission. (2016). Consumer Sentinel Network Data Book. Washington: Federal Trade Commission.

Flamme, M., & Greave, K. (2015). Serving connected customers: How merchants and payment providers can win in a digital world. New York: PWC.

Fox, S. (2009). Privacy, Security and Confidentiality. Informatics for Consumer Health: Summit on Communication, Collaboration, and Quality. Pew Internet & American Life Project.

Gemalto. (2017). Poor Internet Security Takes its Toll. Belcamp: Gemalto; SafeNet.

Germalto. (2017). Breach Level Index. Belcamp: Germalto.

Herrero, A., & Lopez, G. (2010). Access to Information and Transparency in the Judiciary. Washington: Association for Civil Rights.

Larson, S. (2017, December 20). The hacks that left us exposed in 2017. Retrieved from CNN Tech: http://money.cnn.com/2017/12/18/technology/biggest-cyberattacks-of-the-year/index.html

Leape, L. L. (2010). Transparency and Public Reporting Are Essential for a Safe Health Care System. New York: The Commonwealth Fund.

Liang, H., &Xue, H. (2009). Avoidance of Information Technology Threats: A Theoretical Perspective. MIS Quarterly, 71 - 90.

Moorning, K. M. (2013). Information Privacy Challenges in E-Commerce Transactions. International Journal of Computer Science & Information Technology Applications, 1(1).

Parramore, L. S. (2011, November 29). Are You Held Hostage By Bad Credit? The Hidden Truth Behind the Shady Credit Agencies That Can Ruin Your Life. Alternet.

Rasmus, D. (2006). The New World of Work: Transparent Organizations. Redmond.

Smith, S., Winchester, D., Bunker, D., & Jamieson, R. (2010, September). Circuits of Power: A Study of Mandated Compliance to an Information Security de jure Standard in a Government Organization. MIS Quarterly, 34(3), 463-486.

Soha Systems. (2016, May 17). Soha Systems' Survey Reveals Only Two Percent of IT Experts Consider Third-Party Secure Access a Top Priority, Despite the Growing Number of Security Threats Linked to Supplier and Contractor Access. Retrieved from Market Wired: http://www.marketwired.com/press-release/soha-systems-survey-reveals-only-two-percent-it-experts-consider-third-party-secure-2125559.htm

Sorrell, S. (2017). Online Payment Fraud Whitepaper 2016-2020. Hampshire: Juniper Research.

Statistica, . (2017, October). Retail e-commerce sales in the United States from 2016 to 2022 (in million U.S. dollars). Retrieved from Statistica, The Statistics Portal: https://www.statista.com/statistics/272391/us-retail-e-commerce-sales-forecast/

The Open Group. (2014, August 22). What is FAIR? Retrieved March 1, 2018, from The FAIR Institute: https://www.fairinstitute.org/what-is-fair