Developing a Quantitative Framework Tool to Implement Information Security Risk Management

by

Ronald Wilson, Jr.

A thesis submitted to the Information and Logistics Technology,

College of Technology

in partial fulfillment of the requirements for the degree of

MASTER OF SCIENCES

in Cybersecurity

Chair of Committee: Wm. Arthur Conklin, PhD

Committee Member: Chris Bronk, PhD

Committee Member: Denise Kinsey, PhD

University of Houston

November 2019

DEDICATION/EPIGRAPH

This paper is dedicated to my parents & two siblings, son, fiancé, and daughter

ACKNOWLEDGMENTS

I acknowledge my professor and advisor Dr. Conklin. Your guidance, assistance, and brief talks of wisdom help construct and define my paper. My professor Dr. Bronk for introducing a wide variety of cyber resources, newspapers, magazines, journals, etc. Dr. Wilson thanks for setting the challenge to write and take interest in research. I acknowledge my one and only son. Thanks for being who you are and no matter how far our distance you remain in my heart. Last, but not least I thank my fiancé and daughter for putting up with all the days, nights, and weekends of hearing "Sorry, I have to go study."

ABSTRACT

The purpose of this paper is to provide a quantitative cyber risk management framework to implement in small to medium organizations' operational plan. This paper will analyze resources to estimate patterns of attacks, cost of assets, cost of data records, and cost/benefit analysis. With proper calculations, a small and medium business owner will be able to follow the framework and produce two outcomes: annual loss to the organization and cost of benefit estimation to discover return on investment. After these two outcomes one of three decisions will be determined by executives or stakeholders, either accept risk, transfer risk, or invest in risk management.

Table of Contents

LIST OF TABLES

LIST OF FIGURES

CHAPTER I

DEVELOPING A QUANTITATIVE FRAMEWORK TOOL TO IMPLEMENT CYBER RISK MANAGEMENT

Introduction

Risk is the measure of extent to which an entity is threatened by a potential circumstance or event, and typically a function of (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.[i] Considering risk in its transitive verb form, it is an event which places a direct object in jeopardy of being exposed to a hazard or dangerous circumstance. In cybersecurity risk information systems are the direct objects at jeopardy of being impacted by an adverse event. In order to control or mitigate these circumstances, cyber risk management must be implemented as a supporting process to manage information systems security for organizational operations, organizational assets, individuals, and the Nation.[ii]

The purpose of this paper is to analyze previous breach report data and design a fundamental framework model for small and medium organizations to quantify cyber risk management. Developing a base framework for small and medium organizations to implement also sustains an organization's longevity after a cyber-attack occur. Qualitative and Quantitative risk assessment are key elements of implementing risk management. However, both are challenged with barriers due to the lack of resources and skills. Challenges will be discussed in Chapter 2. For the purpose of this paper a quantitative risk analysis will be the key emphasis. To build a framework necessary to analyze and quantify cyber risk management, the following four factors must be present: (1) Asset Value, (2) Data Record Cost, (3) Cost/Consequence Modeling, and (4) Cost Benefit Analysis.

Cyber risk management becomes a challenge for small and medium organizations to implement due to lack of technical skills, resources, and support.[iii] For small and medium organization to efficiently budget an investment in cyber risk controls, a Quantitative framework must be available for the stakeholders and senior management to evaluate cost.

Two common reports are analyzed to cipher cyber data breaches and cost of data breaches. The present paper analyzes the Verizon Data Breach Investigation Report and Ponemon Institute Cost of a Data Breach Report to discover common attack methods, provide estimated cost of breached data records, estimated cost of business and implementing security controls, and cost of cyber breaches within specific industries.

The following chapters will discuss the elements to building and modeling cyber risk management framework. Chapter 3, analyzes data breach reports methodology for Verizon Data Breach Reports and Ponemon Institute Cost of Data Breach Reports. Chapter 4, relates the Bowtie Model Analogy to build a cost analysis of security controls to mitigate or apprehend an attack. Chapter 5, analyze data results to build patterns of attacks, cost of data records after a cyber breach occur, and building the quantitative framework. Chapter 6, presents the three step Cyber Risk Management Framework Model and a complete walk through of the process. In conclusion, Chapter 7 summarizes the complete Cyber Risk Management Framework concept and outcome.

CHAPTER II

CHALLENGES OF CYBER RISK MANAGEMENT

To establish the context of risk-related activities, challenges of small and medium organizations must be acknowledged. Collectively, challenges throughout organizations include (but are not limited to) financial, technical skill level**,** insurance liability, Regulations not clearly defined, availability of information**,** and neglected employment training.[iv]

Financial Challenge

Organizational operation challenges are aligned with the financial welfare of the organization. Stakeholders and executives are concerned with return on investment before allocating a portion of budget to mitigate cyber risk. Without a clear vision as to how an investment in cyber risk management will alleviate the likelihood of an organization losing revenue, executives may not be willing to invest in cyber risk management budget.

Simon Marvel suggests that financial and technical gap is a hindrance to executives. From a financial standpoint, executives are not as willing to invest in cyber risk management if it does not directly improve their financial goals: earnings growth, sales target, economic value added, efficiency savings and market share.[v]

In the absence of financial support, challenges arise with the inability to purchase updated, eventually leads to legacy equipment. Legacy equipment evolves into multiple disadvantages for Information Technology (I.T.) Professionals. Network weaknesses arise such as software incompatibilities, vulnerabilities from unpatched security ports, or inability to properly configure according to best practices. Therefore, leading to threat exposures. A survey conducted by Ernst Young in 2017 revealed 46 % of 1200 executive participants from organizations around the world were faced with outdated security controls and architecture.[vi] Considering one in ten organizations within that same survey lacks a breach detection program, 75% of respondents rate the maturity of their "vulnerability identification" as very low to moderate. Only 4% considered their organization as fully capable of tracking relevant risks and threats.

Insurance Challenge

Cyber insurance is defined as, "the transfer of financial risk associated with network and computer incidents to a third party…"[vii] Deficient insurance coverage and the reluctance to financially support an organization in lieu of a cyber breach, places strain or liability solely on the organization. One strain an organization encounter, lead to impractical security. Impractical security consists of a network without proper security infrastructure configuration. Further complications include insurers not investing.

Insurance companies are concerned with the "transfer" of financial responsibility. The concern for insurers is, enabling organizations to become dependent on insurers, and neglect efforts of securing their domain and infrastructure first.

Impractical security may become more common as the well-defined gap of responsibility between executives and technical staff reside. In most organizations today, there is distinct gap between business leaders and security teams. Essentially, a disconnect with security teams are absorbed in trying to determine what a cyber incident is and how fast it can be stopped, while the business leaders are laser focused on only the impact to the organization.

These gaps create a substantial risk for insurance companies, because the insurers are not certain organizations have properly implemented security controls to mitigate risk, which results in greater cost to the insurance company and loss in revenue. As a result, insurance companies offer less than optimal coverage and premiums cost rise significantly.

The unpredictable characteristics of a cyber breach is a factor to higher premiums. The lack of data history, progression of technology and complexity of attacks make cyber breaches more difficult to predict and quantify. For instance, between June and November hurricanes are most easily predicted. However, cyber breaches occur dynamically. According to A.M. Best's report, a lack of historical experience and tested cyber exposure models continue to foster uncertainty of underwriting cyber insurance.[viii] Stakeholders and executives are unwilling to invest into insurance policies due to the inability to provide reasonable coverage from such a disaster.

According to the Insurance Journal, the total number of cyber insurance claims, in the U.S. market alone, were close to doubling between 2016 and 2017, from 5,955 to 9,017. This demonstrates the need for more efficient methods of quantifying risk. Completely stopping risk by implementing more cost-effective tools is not a financially effective method.

As insurance claims rise, revenue for security control equipment raised also. In a report from research firm Gartner, cyber risk is causing significant costs to business practices. For instance, they state: "Worldwide cyber-security spending for 2015 topped $75 billion and in spite of this level of spending, we have seen 2000 data breaches, 700 million personal records stolen, and an average financial loss of $3.5M per incident." However, the most shocking statistic is that on average, organizations only know that they have been hacked less than 30% of the time.[ix] In spite of spending more dividends on equipment and software, the cyber breach incidents continue to dominate the networks and cost twice as much financial damage.

Reports show the average cost of cleanup for a cyber breach in a small business is $690,000, and for a middle market companies over $1 million.[x] Collectively insurance companies have suggested the following challenges in providing premium coverage:

- Scarcity of historical data
- Cyber risk is dynamic, and sometimes suddenly and drastically changes due to technical progress and the use of novel systems and devices.
- Laws and Regulation may significantly alter corporate risk management strategies and losses insured under a cyber risk policy, thus posing additional risk to insurers

The spike in Cyber breaches and high revenue cost to recover from a cyber breach have caught global attention of Executive Leaders. Executive Orders, National Laws, and open dialogue have implied an immediate concern for processes and procedures to be implemented in all areas of business.

Four reasons insurance policies cost is driven up: (1) Newness of product and small size of risk pools; (2) Small number of market participants; (3) Limited data, making larger risk; and (4) Require costly state verification and upfront risk assessments.[xi]

After considering the failing efforts in the past to protect against cyber breaches, little confidence remains in a successful defense. Therefore, stakeholders and executives are not investing budget in cyber risk management.

Two reasons smaller organizations find difficulty in implementing cyber risk management plans are the magnitude and complexity of cybersecurity risk, and the investment draw on precious corporate resources[xii]. Cyber breaches frequently changing and creates an uncertainty as to which security method is best to implement. Therefore, insurance companies are not portraying an affordable investment coverage to small and medium organizations.

Financial loss of business and high premiums signifies a demand to continue developing frameworks to influence investing in cyber risk management operational plans. Insurance companies are more willing to cover organizations that have proper planning and contingency plans in place. Planning risk management allow businesses to know what assets are at risk, the value of the asset(s), and plan how to protect, cover, or accept the loss of losing and recovering the asset(s) in a different manner.

Technical Skills Challenges

Skill level is essential to how well risk can be managed by technical staff within an organization. Lacking knowledge and skills contribute to ineffective managed risk and unavailable technical details to assess and mitigate further events.

Advanced skills such as data learning are lacking in small and medium organizations. Larger organizations with budgets of $250 Million and greater are more instrumental in distributing cost for this skill level. Organizations with less than $50 Million are less likely to allocate cost or find reasoning to fulfill these positions.[xiii] Technical professionals are able to track and analyze real time changes to data over time. With this level of insight into the network, technical professionals discover irregular traffic more efficiently.

The ability to trace vulnerabilities, threats and breaches, may lead to accurate historical data of patterns and data breach commonalities. Future predictions and decisions will be based on this historical data. Organizations ability to make future predictions helps stakeholders plan their

operational budget to protect the assets that are most at risk. Protecting assets is a key factor in cyber risk management framework.

One solution to consider for smaller organizations who lack advance skills is to rely on larger organizations to communicate data sharing between organizations. Publicizing information help smaller organizations become knowledgeable of popular patterns, vulnerabilities, threats, and breaches to remain informed and updated to adjust and improve skill technical levels. If technology is not improved, results evolve into outdated technology and staff not motivated to engage in learning new skills. Stagnant skill growth is another result in legacy technology and inefficient practices. Ultimately, this technology will no longer be supported or updated with proper security patches, vulnerabilities, and weaknesses created in the network.

A second technical challenge relates to executives and technical personnel difference of viewpoints. Confounded terminology between financial and technical personnel result in unproductive outcomes. Therefore, executives will not support the financial obligation of implementing time and budget to support an unconceivable plan. This language gap hinders information systems advancement and attaining proper security. The development of a universal language is necessary to build a bridge for understanding between the two parties.

Ekelhart et.al [14][xiv] states that common, logical and effective understanding of the fundamental Information Systems (IS) problems are required in order for the IS profession to evolve significantly. Risk-based Cybersecurity Framework is the National Standard which provide common language for all organizations.[xv] National Institute of Standard Technology (NIST) framework was developed by international small and large organizations, with guidance from NIST. These standards and guidelines from NIST will be referenced throughout this paper to build a framework for quantifying risk management.

Regulations Not Clearly Defined

State and federal laws are not clear regarding responsibilities of cyber breaches. Unlike the European Union that operates under one governed law (the General Data Protection Regulation), each state within the United States governs cybersecurity responsibility individually.[xvi] With jurisdiction boundaries within the same Nation, limited power exists when prosecuting across

borders, which erect a major concern. Attempting to hold a person responsible for an act which is not enforced by law enforcement in another jurisdiction eliminates the necessary power and control to investigate and prosecute an offender.

States pursuing such strategies will inevitably face dilemmas regarding who and what to prioritize and how far to go in their defense.[xvii] The borderless nature of cyberspace raises legal and ethical questions for governments. Should the state accept responsibility for defending networks and computers of its companies that lie outside of its territory? Should it defend those of foreign owned companies or multinational corporations located within its territory? Should it extend its defense to cloud-based assets? Will organizations with less restrictions become relax in securing networks? These questions pose concerns to how regulations differ and can cause controversial circumstances.

Availability of Information

Too commonly managers, executives and stakeholders are disjointed between each other, concerning an organizations' risk management plan. Questions continue to rise amongst stakeholders who feel there has been no clarification regarding cyber risk management. Olga Botero, Director of Evertec Inc. and Founding Partner, C&S Customers and Strategy expressed, "There are still many questions unanswered for boards, including: How good is our security program? How do we compare to peers? There is a big lack of benchmarking on practices."[xviii]

Stakeholders are dissatisfied with the quality of management related to cybersecurity information. To grasp a better understanding of the technical demand to control data breaches, stakeholders desire to see Key Performance Indicators (KPI) in alignment with the business plan for the organizations. Measurable goals with clear objectives enlighten how cyber risk management plans align with organizations business plans. By quantifying data breaches according to the various companies cost of informational data records compromised, over time organizations are able to measure the company's performance and progress toward meeting a goal. With the ability to observe data breach outcomes for an extended time period (i.e. one-year, three-year, five-year benchmarks), Key Risk Indicators (KRI) can be measured to determine how frequent an activity occur and its level of risk to the organization. Without

transparency of comprehensible information, benchmark reports will not show progress or return on investment.

Neglecting Employment Training

Employees are key targets to security within an industry's network. Today's industry consists of thousands of endpoints, with majority controlled by employees. Each endpoint is an entrance of opportunity for an attacker to enter the network. This creates an overwhelming approach to protect an organizations' network. Information security training is for both technical staff and non-technical. Presenting relevant training is the key to both groups.

Technical staff must remain trained and updated on new equipment and best practices. After conducting a study by Information Systems Security Association (ISSA) and analyst Enterprise Strategy Group (ESG), a survey of 343 cybersecurity professionals expressed with 67% agreement, maintaining appropriate training was difficult.[xix] Technology advances on a daily average. These advancements create innovative ways not only for communication but security. As legacy technology has already been discussed as a concern, it is important to mention its inability to remain updated and patched to new threats and vulnerabilities. New methods and configuration solutions will be implemented to accommodate new threats. Learning in the field of technology cannot be adjourned. It must be considered as a professional goal and attained through continuing education, certification, and experimentation.

Non-technical staff may be trained on how to identify threats and the common tactics used to lure them into a security breach. With knowledge staff become more susceptible to why and how certain practices are imperative. Employee training not only enlighten awareness for in office but home and public locations as well. Training should be interactive and relative to non-users.

Ponemon Institute results reveal that training employees was the most popular method of mitigating breaches between 2009-2015, averaging 54%. In 2019 reports confirmed employee training reduced total cost of data breaches in the United States by $270,000 dollars. However, in small and medium organizations, operational budget and lack of insight still hinder training for both technical and non-technical staff. Surveys conducted by ISSA and ESG reveals 38% of

cyber professionals' organization do not invest in appropriate training. With such a deficiency in training, smaller companies are used as stepping stones to larger companies.[xx] Attackers target these companies as entrance points and wait for the opportunity to connect to larger companies when the opportunity presents.

As networks are setup to interact with customer services, smaller organizations allow third party companies access into their network through remote applications. Services such as air conditioning HVAC or security camera monitoring, use remote connections to access equipment on the network. The smaller companies who provide these services are infected first. Once connected to the inside of a larger companies, an attacker pivots their way onto the larger company's network. Remote access is just one way of forced entry to larger networks.

Challenges exist and create many obstacles for non-technical, technical, managers, executives, and stakeholders. Some issues overflow into state, national, and foreign issues. These challenges have been identified globally and market a concern for numerous organizations. Knowledge and experience will be the key to mitigating risk over time.

CHAPTER III

DATA BREACH REPORTS METHODOLOGY

Verizon Data Breach and Ponemon Institute Cost Data Breach reports are referenced throughout this paper to analyze attack patterns, common attack methods, commonly attacked assets, cost of data breaches, and individual industry loss of business. Losses related to asset value, and the frequency rate of an occurrence help identify the first step of the quantitative framework (details in chapter VI). Cost of data records will quantify the second step of the framework. These two major breach reports stand out when considering breach details. For the past decade historical data from forensic investigations and partnerships have been reported using a consistent methodology, industry target commonalities, and reports from both Nationwide and Global breaches. Other data breach reports such as Symantec Internet Security Threat Reports and Microsoft Security Intelligence Reports include information similar, but based from these reports.

With these two reports filtering majority of data, a synopsis of information can be gathered to help quantify assets and data records. Analyzing and organizing data will identify patterns in threats, vulnerabilities, and breached data records related to specific industries. Within these industries cost of records and assets can be estimated. Both Verizon and Ponemon Institute reported similar industries as targeted attacks involving breach attempts and compromised data. Differences in reports help complement each other to relate breach attack patterns and cost.

Verizon Data Breach Reports

Early Verizon Data Breach reports were analyzed by the Verizon Business RISK team and less than twenty contributors. They begin recording data breach incidents in 2004. As reports became more consistent, by 2019 seventy-three contributors submitted data incidents and breaches. In 2010 reports, United States Secret Service (USSS) developed a partnership with Verizon to globally enhance the scope of data breaches. With a global presence, by 2016 Verizon reports grew to include 82 countries.

Methodology

Verizon reviews all incidents and converts them to the Vocabulary Event Recording Information System (VERIS) framework. The basics of the framework include three methods:

1. Direct recording of paid external forensic investigations and related intelligence operations conducted by Verizon using the VERIS Webapp
2. Direct recording by using VERIS
3. Converting partners existing schema into VERIS

The VERIS Webapp Java Script Object Notation (JSON) and spreadsheets are placed within an automated workflow that converts the incidents and breaches into the VERIS JSON format (if necessary). Missing enumerations are added and then records are validated against business logic and VERIS schema. The automated workflow subsets the data and analyzes the results. Based on the results of the exploratory analysis, the validation logs from the workflow and discussions with the partners providing the data, is cleaned and re-analyzed. This process runs nightly for roughly three months as data is collected and analyzed.

Cyber breach incident's eligibility is classified and separated into subsets. The baseline of an entry must be confirmed as a security incident, which entail a loss of confidentiality, integrity, or availability. Once the baseline of an entry is met, an assessment to filter the incident is completed. The "quality" of a filtered incident consists of:

1. The incident must include at minimum seven enumerations (e.g. threat actor variety, threat action category, variety of integrity loss, etc.) across 34 fields, or be a Distributed Denial of Service (DDoS).
2. The incident must have at least one known VERIS threat action category (hacking, malware, etc.)

All incidents must be in timeframe of the analysis between November 1 to October 31.

Data subsets are incidents which pass the "quality" filter requirements mentioned above. In addition to normal filtered incidents, separate categories are created to analyze data which would obscure smaller trends (i.e. botnets).

Limitations

Verizon does not claim to include all data breach occurrences. Records are combined from contributors consisting of isolated incidents. Many breaches go un reported and are not included. Therefore, Verizon's confidence in their statistical data ranges from +/- 0.4% for incidents and +/- 2% for breaches, averaging about 95% confidential rate.

Ponemon Cost Data Breach Reports

Ponemon Institute states their study focus pertains a business process and not data protection or privacy compliance. Their goal is to calculate the cost of a data breach. The methodology behind their study is related to activity-based costing (ABC). This method identifies cost and assigns a cost based on actual usage. Activity Based Costing involves an approach to the costing and monitoring of activities, which involves tracing resource consumption and costing final outputs[xxi]. ABC is driven by cost drivers, which are the activities that cause costs to increase.

Figure 1. The Activity-based costing process:

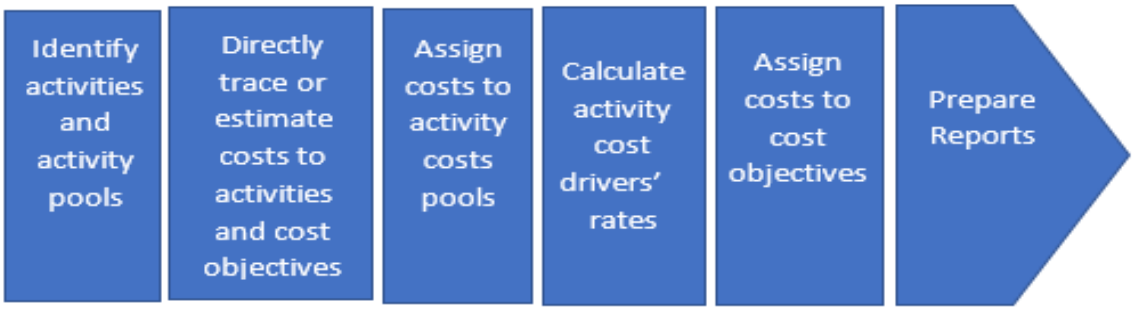

Figure 1 The Activity-based Costing Process

Cost is based on estimates provided by companies who determine the cost of activities necessary to resolve a data breach. Two categories are considered when estimating costs of these data breaches. Immediate Response to a data breach and Aftermath Response:

Immediate response consists of:

- Conducting investigations and forensics to determine the root cause of the data breach
- Determining the probable victims of the data breach
- Organizing the incident response team
- Conducting communications and public relations outreach
- Preparing notice documents and other required disclosures to data breach victims and regulators
- Implementing call center procedures and specializing training

Aftermath responses consists of:

- Audit and consulting services
- Legal services for defense
- Legal services for compliance
- Free or discounted services offered to victims of the breach
- Identity protection services
- Lost customer business based on calculating customer turnover
- Customer acquisition and loyalty program costs

Once the estimates are provided for the Immediate and Aftermath responses, costs are categorized as Direct and Indirect. Respectfully direct expenses outlay to accomplish a given activity and indirect expenses is the amount of time, effort, and other organizational resources allocated to a data breach resolution, but not always a direct cash expenditure.

Data Collection Methodology

Ponemon's data collection methods relies on a numerical estimation based on the knowledge and experience of each participant. Benchmark incidents rate direct cost estimates for each cost category by marking a variable range in a number line format. To preserve confidentiality each participant was asked to mark a number between the lower and upper limits of a range for each data breach cost category. Cost were limited to known ranges pertaining to business operations who handle personal information.[xxii]

By 2019, Ponemon reports were conducted from 507 organizations, 16 countries or regions, and between 2,000 to 100,000 breach records. Seventeen industries were included in reports which contained records and information stored on assets within the organization, or from a third party's network with remote access.

Limitations

The majority of organizations are considered to have mature privacy or information security programs formed with personnel who directly deal with cost revenue and budgets. This insinuate most organizations surveyed were financially stable and advanced organizations. Ponemon Reports lack scientifically driven methods; therefore, it has acknowledged an error rate of confidence cannot be provided. Limited participants do not represent the entire number of breach occurrences, therefore unreported cost may differ for some industries. Cost inaccuracy may also be a result of inaccurate reported costs. However, Ponemon does perform checks and balances for each benchmark processed. Each breach currency rate is converted to U.S. dollars resulting in possible local deflated costs.

CHAPTER IV

BOWTIE MODEL ANALOGY

The Bowtie Model is used to identify, assess and analyze the cost/benefit of an organization's assets and controls.[1] First it identifies the Critical Event (known as Top Event) which may threaten the organization's confidentiality, integrity, or availability. Second, it assesses the organization causes, consequences, and barriers which leads to a critical event. In conjunction, the bowtie model exposes possible results and controls to mitigate the critical event. Finally, it directly leads to an organizations cost/benefit calculation, which factors into the conclusion of the quantitative framework. Models are a dynamic and inclusive way to gather information and make decisions.

Models help provide compact clean visuals to specific details. The relationship between the flow of models and applying a concept help identify more concise overall significance and compact details. The Bowtie model method is more common in safety industrial fields such as oil & gas, chemical, aviation, or mining. These industries use four basic methods of the model to protect or mitigate a catastrophic event occurring:

- Top Event (Critical Event)
- Fault Trees
- Event Trees
- Barrier thinking.[xxiii]

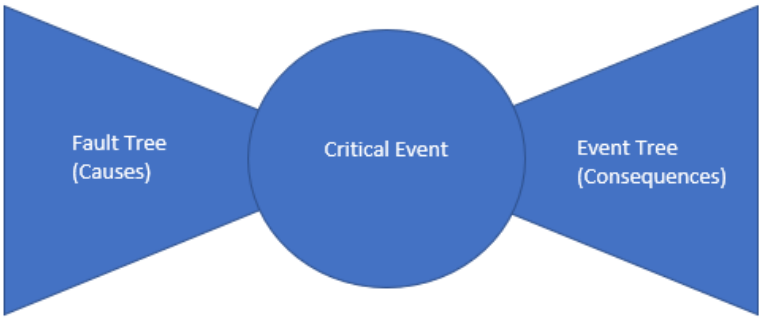

Figure 2 Bowtie Model Structure

[1]It's Origination stem from an early version of the fault tree and leading to the event tree. This method was developed by Nielsen (1971). Nielsen described the critical event as a 'transgression of the safety limit of vital reactor parameter'. (IADC, 2010, Health Safety and Environment Case Guidelines for Mobile Offshore Drilling Units. Tech. Rep. International Association of Drilling Contractors, Houston)

The Bowtie Model in Figure 2 replicates Nielsen's cause and consequence diagram. Today it has transformed into the four methods discussed below. Once all four methods are complete, a quantitative analysis can be determined. This analysis will extend into determining how risk is managed. Executives and stakeholders of an organization will assess the barriers in place and determine if the return on investment to is greater than the loss resulting from the Critical Event occurring.

Method 1: Top (Critical) Event

The Bowtie Model is a diagram used to present a critical moment of failure in the system. It is centered around a Top Event. This point of the diagram represents the moment control is lost.[xxiv, xxv] For purposes of this framework the Top Event will be referred to as Critical Event.

Critical Events are known as the common junction connecting major "causes" and "consequences" contributing to a specific point of failure. Several pathways are created starting from the Critical Event and extending outward. Possible "Causes" of the Critical Event are listed to the left of model. Resulting "Consequences" are listed to the right of model. These two analogies present the comparison of causes and consequence to exhibit before executives and stakeholders who make decisions of the organization's investment budget. Executives and stakeholders reconcile rather their final decision to invest is more profitable than accepting the risk and enduring consequences.

Method 2: Fault Tree

The Fault Tree refers to the "Causes" or possibilities which may occur leading to a critical event. These events include any vulnerability or threat which exposes the organization to a Critical Events identified in Method 1. A fault tree magnifies how well the organization is currently prepared to prevent or manage risk and what policies and/or controls are in place. Typically, "Fault Events" can be read from left to right enumerating "Causes" (threats & vulnerabilities) leading to a "Critical Event".

Vulnerabilities and threats can initially be determined from Verizon Data Breach Reports. Internal technical staff, if available, can provide insight from self-initiated vulnerability scans or a third-party assessment can be acquired. Each fault (cause) should be identified and listed for consideration.

Method 3: Event Tree

The Event Tree represents "consequences" which result from the Critical Event occurring. Once the critical event has transpired the consequences are resulting factors from this specific event. Therefore, the Event Tree typically expands to the right of bowtie listing these results. Reading the events from left to right indicates the Critical Event occurring first, then consequences evolving into possible outcomes following afterwards. Events may be listed in any order.

The current paper extract consequences from both Verizon and Ponemon Reports to be analyzed in this study. Results such as cost of replacing assets, downtime, customer turnover, loss of business income, cost of records, direct and indirect cost, fees, branding, etc. are estimated outcomes from both reports. However, internal business managers, executives, and technical staff may add or reduce possible consequences depending on business needs. Each consequence is normally attached to an estimated cost. These results help drive the quantitative outcomes and calculate the Annual Loss Expectancy.

Method 4: Barriers

The ultimate goal is to mitigate the Critical Event from occurring. Business continuity and resilience are its key factors. According to Sklet, "There is no universal and commonly accepted definition of terms like safety barrier…" He proceeds to define safety barriers as, "Physical and/or non-physical means planned to prevent, control, or mitigate undesired events or accidents".[xxvi] Protecting an information system from a catastrophic Critical Event entail setting information security controls in place to govern such events. These controls consist of policies, procedures, best practices, software or hardware to monitor and identify "causes" from occurring, or how to leverage "consequences" after the Critical Event occur.

One of three reasons that de Dianous and Fiévez imply to implement barriers, is to help identify areas that are not sufficiently controlled yet.[xxvii] Current barriers which already exist, help identify "cost/benefit" for the organization and reduces the overall cost of Annual Loss Expectancy. Barriers not in place become possible investments for executives and stakeholders to invest. With dynamic change in technology, barriers can constantly be updated as the organization grows and develop new technology. Re-assessing the needs of the organization is a priority.

Within the Bowtie Model, barriers are placed between each "Cause" or "Consequence" leading to and from the Critical Event. From the Fault Tree barriers represent security controls set in place to mitigate a threat from occurring. Barriers placed on the Event Tree side represent security controls or policies to mitigate certain consequences following a critical event. Barriers are flexible and may be used to mitigate more than one "cause" or "consequence".

Applying Bowtie Model to Cyber Risk Management Framework

Quantitative Cyber Risk Analysis relies on four steps of the Bowtie Model to calculate cost for an organizations budget. Barriers identified throughout the model are heavily relied on to assess the organizations current security controls in place to withstand a critical event. Cost is then determined based on cost of barriers unmet, asset value, and estimated costs of data records compromised.

In order to develop estimated costs Operational Security processes will be used to build our bowtie model. Operational Security is a military analytical process that classifies information assets and determines the controls required to protect them. Five steps are correlated to prevent potential adversaries from discovering critical operations-related to data; (1) Identify critical information, (2) Determine threats, (3) Analyze vulnerabilities, (4) Assess risk, and (5) Apply appropriate countermeasures.[xxviii] These five steps will be implemented to identify the four methods of the bowtie, and determine the controls required to protect or mitigate a critical event from occurring:

I. **Step 1. Identify critical information**: Determine what assets and data are most important to the organization.

II. **Step 2. Determine Threats:** Determine what threats are critical to an organization's assets and data. Verizon Data Breach Reports classify four types of threats. Two of the four threats to help build the bowtie model are "Threat Agents" and "Threat Actions". Threat agents refer to entities that cause or contribute to an incident. They are best classified by three categories including, internal, external, or as a partner. Threat actors determine what method the attacker used to accomplish the breach. It describes what the threat agent did to cause or contribute to the breach. These are normally broken into seven categories:

    1. Malware
    2. Hacking
    3. Social
    4. Misuse
    5. Physical
    6. Error
    7. Environment

III. **Step 3. Analyze Vulnerabilities:** What weaknesses are in jeopardy of allowing threats to penetrate critical assets and compromise data identified in Step 1? Third - party assessments are commonly used to determine vulnerabilities.

IV. **Step 4. Assess Risk:** Assess the vulnerabilities identified in Step 3. Determine the level of threat associated with each of them and how damaging an attack would be to the organization continuity and loss of finances.

V. **Step 5. Apply appropriate countermeasures**: Implement a plan to mitigate the risks. This involves identifying controls to protect and mitigate risk identified. List both current and necessary barriers to fulfill requirements. Technical staff or third party is recommended for consultation.

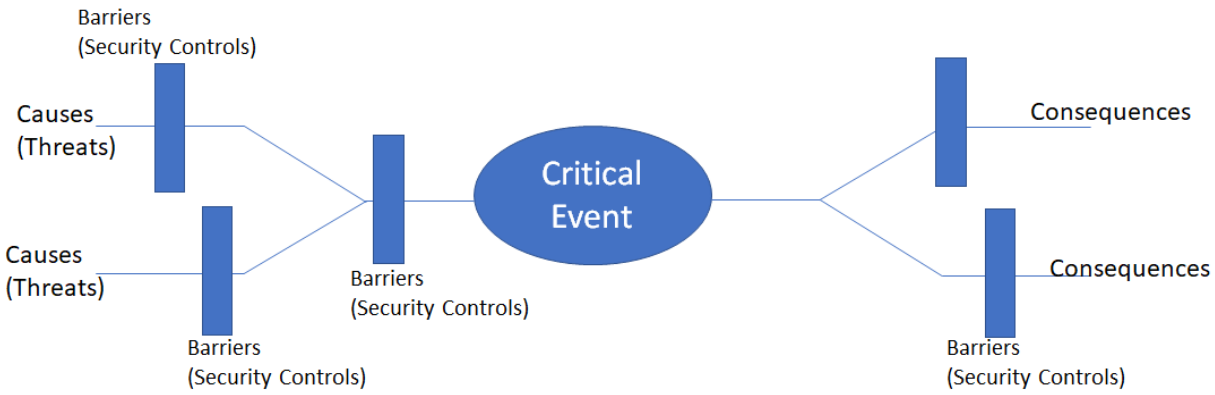

Figure 3 Bowtie Diagram

Once steps are completed, the bowtie model should present a diagram structured similar to Figure 3, including scope of critical events, threats or vulnerabilities, consequences, and security controls. This scope is quantified using cost/benefit calculated estimates. The cost of existing security controls is taken into consideration. Once the necessary controls are incorporated into the model and cost is identified the quantitative analysis along with cost/benefit calculations is ready to be completed and presented to executives and stakeholders for decisioning.

CHAPTER V

ANALYZING DATA RESULTS

To build a quantitative framework for cyber risk management, an analysis of patterns and data records cost must be identified. Patterns will identify which assets are targeted (Assets) and what action affected the asset (Actions). Early Verizon Data Breach Reports refer to the four A's to represent the minimum information necessary to describe an incident or threat scenario.[xxix]

Table 1 The Four A's

Actors	*Whose* actions affected the asset
Actions	*What* actions affected the asset
Assets	*Which* assets were affected
Attributes	*How* the assets were affected

With the four A's an incident can be structured to measure frequency, identify controls which protect or mitigate a breach, and associate impact to an incident or breach.

As previously mentioned, in the absence of multiple decades of prehistoric data, cyber risk management is difficult for most organizations to construct. Patterns and trends derive from analyzing historical data, which make identifying frequency rates and forecasting attacks possible. Verizon and Ponemon Institute have constructed reports and gathered data consistently for the past decade. The following reports will be analyzed accordingly:

Verizon Data Breach Reports:

- Identify patterns of incidents associated to specific industries
- Identify targeted assets
- Identify types of attacks
- Identify targeted data

Ponemon Institute Reports:

- Identify cost of breach to an organization
- Identify cost of breach to assets
- Identify cost of breach to data records
- Identify cost of breach associated with specific industries

Common Industry Data Breaches

Verizon Data Breach reports have categorized incidents and breaches into seven categories based on common threat actions. These seven actions can be categorized into nine patterns of attacks. These seven actions will be discussed in detailed, but first it is important to analyze how Verizon attained and categorized these nine patterns.

Verizon conducts machine learning on incidents over time, which allows them to discover and categorize the nine patterns mentioned above. Machine learning is an intricate scientific program learning language which arithmetically organizes data based on features and labels. These features are organized by running arithmetic codes to classify or cluster data, until a pattern becomes constant and does not change. It is a very high processing procedure which is capable of analyzing a plethora of information captured from a data source in a matter of hours. These technical skills are not performed in an average day's work, but is a dedicated time-consuming skill, usually performed by a third party or a large corporation such as Verizon.

Verizon uses the four A's to find recurring combinations of actors, actions, assets, and attributes. To expose dormant patterns, the Verizon for Event Recordings and Incident Sharing (VERIS) team applies a statistical clustering technique by creating a matrix accumulating incidents within each of the common VERIS enumerations and calculations. The distance is then calculated between each enumeration and incident. This allows grouping of clusters or patterns strongly related to VERIS enumerations within the incident dataset. The relationship between an incident and an enumeration must be distinct from other combinations. VERIS looks for clusters to describe comprehensive incident classifications versus frequent pairing. Once a pattern has been identified, such as an ATM attacked by an organized criminal group to steal credit card

payments, the pattern is labeled “skimmers”. The incident is removed and cluster re-ran to analyze the remaining incidents and enumerations. [xxx]

In conclusion VERIS discovered nine patterns which confirmed 94% of data breaches collected in 2013. These nine patterns are used in the Verizon Data Breach Reports to describe the frequency rates at which they occur from reported incidents:

1. Point of Sale (POS) Intrusion
2. Web Application Attacks
3. Insider Misuse
4. Physical Theft/Loss
5. Miscellaneous Errors
6. Crimeware
7. Card Skimmers
8. DoS Attacks
9. Cyber-espionage

In 2010 VERIS identified seven primary threat actions:

1. Malware
2. Hacking
3. Social
4. Misuse
5. Physical
6. Error
7. Environmental

Using these established patterns, stakeholders and executives should be knowledgeable of cyber threats and the targeted asset(s). Each organization is able to concentrate primarily on which pattern of incidents are significant in their industry. Executives will be able to calculate the Return on Investment and make clearer decision of whether budget is cost effective to invest.

Two choices are applicable to managing risk after identifying a pattern of attacks and the threat actions associated to an event; one makes a decision to invest, or two not invest in applying controls to mitigate risk. For instance, a smaller organization whose data does not consume Personal Identification or proprietary information decide not to invest in the most expensive network equipment or technical services to protect their data. However, they may budget to replace equipment in case an attack occurs. On the other hand, larger organizations (i.e. healthcare organizations) data may contain millions of health records along with research and costly data. Management may make the decision not to invest in technical services, but instead purchase expensive equipment in addition to an offsite data center to store data and disaster restore systems. These can be used to connect and restore access while replacing infected equipment on location.

Unskilled technical managers may not have the expertise to implement necessary controls or network design. However, from the examples above, allowing an opportunity to have insight on which threats are most significant to their organization, allows the best decision for the resilience and continuity for the organization.

Table 1 provides a description for each of nine patterns listed above. These terms label the attack patterns used to breach data, followed with a brief description, and the industry targeted by this attack.

Table 2 Descriptions of 9 Patterns (Categories)

Pattern	Description	Industry
Crimeware	Malware that did not fit into a more specific pattern. Majority of incidents are opportunities in nature and have financial motivation. Affects consumers and where "typical" malware infections will land	▪ Public ▪ Information ▪ Finance
Cyber Espionage	Incidents include unauthorized network or system access linked to state-affiliated Actors (who) and/or exhibiting the motive of espionage (spying)	▪ Public ▪ Information ▪ Manufacturing
Denial of Service	Any attack intended to compromise the availability of networks and systems. Includes both network and application attacks designed to overload systems, resulting in performance degradation or interruptions of service	▪ Gaming ▪ Information Technology ▪ IT Services ▪ Financial
Insider and Privilege Misuse	Any unapproved or malicious use of organizational resources. This is mainly insider-only misuse (due to collusion) and partners (because they are granted privileges) show up as well.	▪ Public ▪ Healthcare ▪ Finance
Miscellaneous Errors	Incidents where unintentional actions directly compromised a security attribute of an information asset. (does not include loss of devices)	▪ Public Health ▪ Information ▪ Healthcare
Payment Card Skimmers	All incidents in which a skimming device was physically implanted (tampering) on an asset that reads magnetic stripe data from a payment card (e.g. ATMs, gas pumps, POS terminals, etc.)	▪ Finance ▪ Retail
Physical Theft and Loss	Any incident where an information asset went missing, whether through misplacement or malice	▪ Public ▪ Healthcare
Point of Sale Intrusions	Remote attacks against the environments where card-present retail transactions are conducted. POS terminals and POS controllers are the targeted assets.	▪ Accommodations and Food Services ▪ Retail
Web-Attacks App	Any incident in where a web application was the vector of attack. Includes exploits of code-level vulnerabilities in the application as well as thwarting authentication mechanisms.	▪ Finance ▪ Information ▪ Retail

Seven Primary Threat Actions

In concordance with the nine pattern of data breaches the seven most common attack threat actions are important to understand. The four A's, also referred to as Threat Agents, are how the nine patterns derived and formed a pattern during VERIS clustering techniques. Threat agents are summarized to provide information about who (Actors), what (Assets), how (Actions), and why (Attributes) incidents occur.

Verizon for Event Recordings and Incident Sharing, focuses on industries and the attack method an industry may be susceptible too. Data was captured in a Table 3 from Verizon reports, relating the nine attack patterns with an industry. Each industry is followed with a North American Industry Classification Standard (NAICS)[xxxi] code to identify which organizations correlate to this industry.

Table 3 also relates the threat actions most common to an industry per year. These threat actions will be used in quantitative assessment and applied by estimating cost of controls, assets, and records at risk. Organizations are associated with the industry and NAICS code to quickly see what attack method threatens their organization. The first two digits of NAICS code will populate a list of common industries classified to specific codes.

Table 3 Most Common Pattern per Industry

	2012	2013	2014	2015	2016	2017	2018
Crimeware	N/A	Construction (23)	Public (92)	Public (92)	Healthcare (62)	Healthcare (62)	Professional (54)
Cyber Espionage	N/A	Mining (21)	Manuf. (31-33)	Manf. (31-33)	Manf. (31-33)	Public (92)	Public (92)
Denial of Service	N/A	Management (55)		Finance (52)	Information (51)		Professional (54)
Insider Privilege and Misuse	N/A	Real Estate (53)	Mining	Healthcare (62)	Healthcare (62)	Accom. (72)	Healthcare (62)
Miscellaneous Errors	N/A	Administrative (56)	Healthcare (62)	Public (92)	Healthcare (62)	Healthcare (62)	Healthcare (62)
Payment Card Skimmers		Finance (52)	Finance (52)	Finance (52)	Finance (52)	Retail (44-45)	Finance (52)
Physical Theft Loss	Finance (52)	Healthcare (62)	Other Services ()	Healthcare (62)	Healthcare (62)	Healthcare (62)	Healthcare (62)
Point of Sale	Finance (52)	Accom. (72)	Accom. (72)	Accom. (72)	Accom. (72)	Accom. (72)	Accom. (72)
Web Attacks	Finance (52)	Information (51)	Information (51)	Finance (52)	Finance (52)	Information (51)	Retail (44-45)

Note:

- Accommodation = Accom.
- Manufacturing = Manf.

Identifying Assets

After understanding the patterns and threats which target the organization, identifying assets is the first step in cyber risk management framework. This also correlates with NIST Cybersecurity Framework standards.[xxxii] Understanding what is at stake in your organization is the most supportive piece of information for executives and management to determine. This leads to the ability to financially assess the initial cost of assets.

Understanding the cost of assets determines the level of value for an asset. Today, most information is digitized in some form. Digital information become the valued asset, whether it reside within an on-premises computer, electrical device, or a third-party's cloud network. Therefore, cost of asset is determined by the valued information stored on the asset, normally consisting of data records containing the organization's most important information. This information may range from proprietary research, client files, credit card transactions,

demographics of services, patient files, etc. Without this information, the organization daily operations would come to a halt or cause significant revenue loss when not available.

Cybersecurity's initial concern is the protection of data. The value of this information is compounded by its dependence on other assets to function properly. For instance, staff members who assess client's behavior normally enter data from a laptop or computer connected to the internal network. Each local connection within a network is a pathway into the network. That computer or device becomes a targeted source by attacker. The actor who seeks to compromise these devices desire to cause disruption of the network, theft, or destruction to an organization's asset.

The ability to identify assets susceptible to attacks helps eliminate planning and budgeting for objects of less concern. For instance, a staff member's laptop may be stolen. If this laptop is protected with a company password, encrypted files, and requires password to access the network and database records, proper controls have been selected and the cost of asset is narrowed down to replacing the device itself. However, if the laptop contains no security controls and is lost or stolen, not only is the cost of laptop calculated, but the value of each record which may be compromised from the laptop becomes an additional cost along with direct and indirect cost repercussions (i.e. lawsuits by private parties for improper security controls in place).

Executives and management are only concerned with assets that are significant to the operations of the organization. Without proper insight on what is at risk, managing risk will be ineffective and more costly. These decisions are made after compiling all assets and analyzing threats applicable to the environment. Cost of assets are a determining factor for stakeholders and executives deciding whether to accept loss or invest in protecting its value. The final investment decision is based on the assets rate of return compared to financial loss the organization experience from a critical event.

After gathering data from Verizon reports, the seven threat categories can help predict what is at risk. These seven threat categories will be refenced throughout reports going forward. The original seven threats are compiled in Table 4 from 2009 Verizon Database Report:

Table 4 Description of Seven Threats

Hacking	Malicious actions against an informational system
Malware	Captures, stores, and sends data to a remote entity, or enables remote access to a control of the infected system
Misuse	Use of organizational resources and/or privileges for any other purpose than for that which it was originally intended
Deceit/Social	Use of deception or misrepresentation to exploit people, security measures, procedures, or anything that furthers the goal of data compromise
Physical	Lost or theft of an asset, system access, tampering, wiretapping, over the shoulder observation, assault or threat
Error	Only errors directly caused or significantly contributed to a compromise; poor decisions, omissions, noncompliance, and process
Environmental	Catastrophic behaviors such as storms, fires, tornadoes, hurricanes, etc. etc.

As previously stated, information becomes the valued object targeted by attackers. Each of the seven threats may affect the confidentiality, integrity, or availability of a data record. Once the target asset has been identified, the number of records in jeopardy of being affected quantify the total loss involved after a data breach occurs. Calculating the cost per record reveals a portion of budget necessary to recover from loss of data or downtime. Other cost will be considered later.

Understanding assets at risk and threats which target specific data, executives and management will present clear recommended security controls to mitigate risk. As an example, consider a mental organization inability to access data records to a patient database. Without access to a database, the company may lose "x" amount of dollars per day. Each day the records which are not accessible to the organization is unable to properly administer patient care (i.e. medicine dosage amount, allergic reactions, emotional disturbance, etc.). Mitigating the cost of this critical event becomes relevant to the organization at this point. Decisions such as purchasing an off-site service and renewing annual fees versus losing data and not having access for an extensive amount of time becomes important. Stakeholders and executives must make this decision for the benefit of the entire organization.

Table 5 identify the annual percentage of the seven most frequent threat actions occur. In earlier reports the actions were related to records lost in data compromises. Reports after 2014 begin to relate these seven threat actions to compromised data pertaining to different industries. Tailoring reports to reflect threats according to specific industry allow executives to predict the percentage of records exposed during a critical event.

Table 5 Breaches Per Year

Years	**2008**	**2009**	**2010**	**2011**	**2012**	**2013**	**2014**	**2015**	**2016**	**2017**	**2018**
Total Breaches	**90**	**141**	**761**	**855**	**621**	**1367**	**2122**	**2260**	**3156**	**2608**	**2396**
Total Record loss (Approx.)	**285 Million**	**143 Million**	**3.8 Million**	**174 Million**	**44 Million**						
Hacking Caseload	64%	40%	50%	81%	52%			66%	31%	36%	33%
Hacking Record Loss	94%	96%	89%	99%							
Malware Caseload	38%	38%	49%	69%	40%			53%	27%	21%	17%
Malware Record Loss	90%	94%	79%	95%							
Misuse Caseload	22%	48%	17%	5%	13%			8%	7%	8%	9%
Misuse Record Loss	2%	3%	1%	1%							
Deceit/Social Caseload	12%	28%	11%	7%	29%			30%	22%	11%	21%
Deceit/Social Record Loss	6%	3%	1%	37%							
Physical Caseload	9%	15%	29%	10%	35%			4%	4%	8%	2%
Physical Loss	2%	1%	10%	1%							
Error Caseload	68%	2%	1%	1%	2%			8%	7%	13%	15%
Error Record Loss	0%	0%	1%	1%							
Environmental Caseload	0%	0%	0%	0%	0%			0%	0%	0%	0%
Environmental Record Loss	0%	0%	0%	0%							

Cost of Data Breaches

Ponemon Institute provide case studies covering costs an organization incur when responding to data breaches. Primarily, IBM and Symantec Cost of Data Breach Studies are analyzed for this paper. Different versions of Ponemon are published including but not limited to: Cost of a Data Breach U.S. Report, Cost of Data Breach Global Report, and Consumer Study of Data Breach Notification. The resources most referred to in this paper are to identify cost effect of data breaches. Data is analyzed and compiled from Cost of a Data Breach U.S. Report and Cost of Data Breach Global Report.

Ponemon reports take into account the following cost-effective attributes: business costs (including expense outlays for detection), escalation of services, notifications, after-the-fact (ex-post) responses, loss of customer trust or confidence, customer turnover rate, and service rates.

The Ponemon Institute and Pretty Good Privacy Corporation quantifies the actual costs of data breaches for organizations. Estimations are from benchmark surveys released to companies who voluntarily agree to participate. Costs are based on activities resulting from actual data loss incidents. The survey pertains responses to questions an organization would answer when responding to a data breach such as:

- What are the potential legal costs?
- What is industry-average costs resulting from a breach, including the detection, investigation, notification, and possible services offered to affected individuals?
- What are the costs of lost customers and brand damage?
- What are the key trends?
- What measures are taken following a breach that could have been implemented to avert it?[xxxiii]

Ponemon used the shadow costing method to design the survey participants completed. Actual accounting results are not expected, but instead organizations provide broad estimates based on the experience of the subject.

For each category, cost estimation was a two-stage process, direct cost and indirect cost estimates. Respectfully a range variable was used to determine direct cost estimations. The second estimation consist of an opportunity cost estimate provided separately. Calculations are based on relative magnitude of costs in comparison to direct cost within a given category.

How Cost is Calculated

Ponemon uses a core process-related activity which drive the range of expenditures associated with an organization's data breach. The four applied costs include detection, response, containment and remediation.[xxxiv]

1. **Detection or discovery** (detection): Activities that enable a company to reasonably detect the breach of personal data either at risk (data in stored in a location) or in motion (transfer of data).
2. **Escalation** (response): Activities necessary to report the breach of protected information to appropriate personnel within a specified time period.
3. **Notification** (containment): Activities that enable the company to notify data subjects with a letter, outbound telephone call, email or general notice that personal information was lost or stolen.
4. **Ex-post response** (remediation): Activities to help victims of a breach communicate with the company, to ask additional questions or obtain recommendations in order to minimize potential harms. Redress activities also include ex-post responses such as credit report monitoring or reissuing of a new account (or credit card).

The Opportunity Cost Method used by Ponemon is to evaluate the "lifetime value" of the customer to an organization. Data breach costs impact organizations years after a breach occur. Ponemon Data Breach Report 2019 was able to release after effect results for eighty-six companies after a data breach occurred. In their results average costs of breach were 67% within the first year. Second- and third-year breach costs were 22% and 11% respectively.

Data breach costs also relate to customer turnover rates. Current and future customer deficit rates relate to higher cost in an organization's loss of business and placing greater strains if not closure to the organization.

Ponemon relate two categories resulting from these costs:

1. **Turnover of existing customers**: The estimated number of customers who will most likely terminate their relationship as a result of the breach incident. Estimates are annual percentages provided by management during Ponemon's benchmark interview.
2. **Diminished customer acquisition**: The estimated customers who will not have a relationship with the organization as a consequence of the breach.

Based on these categories Ponemon 2019 reports released costs associated to smaller organizations (500 - 1,000 employees) approximately $2.93 million and $204 per record.

Building Quantitative Assessment information from Data Reports

Organizing threats to identify an interference to the organization mission/business are the key point of interest for executives and stakeholders. Utilizing Verizon Data Breach Reports to recognize the trending patterns according to industries concerning their organization will allow technical and management staff to eliminate over bombarding executives and stakeholders with unnecessary information. Four important costs are necessary to help build a quantitative assessment. Using the Annual Rate of Occurrence calculation as a guideline

Table 3 layout the seven major threat actions to compromise data for past ten years. Hacking, Malware, and Deceit/Social threat actions are responsible for 90% of compromised data breaches. Data forensic investigations have consistently identified these threats as root causes to breached data. Four algorithms are calculated to obtain the final Annual Rate of Occurrence (ARO). This rate estimates the potential loss and calculates the rate per year in order to determine the magnitude of the risk, also known as Annual Loss Expectancy (ALE):

1. Find the value and cost of most important assets. Use Verizon Data Breach reports to discover the asset most susceptible to be attacked in your industry. Calculate the Single Loss Expectancy (SLE).
2. Find the average cost of data record to your organization (see Ponemon Reports). Ponemon Data Cost reports can be used to calculate the cost of this SLE.

3. Direct and Indirect Cost will be calculated as an exposure factor. Ponemon Data Cost reports will be used to assist with estimating these costs.
4. Customer Turnover Rate is the second exposure factor to calculate. Ponemon Data Cost reports will be used to calculate this estimate also.

In order for smaller organizations to be knowledgeable of threat actions, larger organizations release specific information detailing attacks and investigations. As previously mentioned in Chapter 2, many smaller organizations do not have finances or skill level to construct intricate levels of investigations therefore larger organization sharing information is able to fulfill gaps of missing information.

Method Processes

Method 1: To understand the pattern of assets an organization is known for being breached, helps organizations quickly identify what and where to look first. For instance, a Purchase of Sale (POS) or Credit Card Skimmer system is known for being attacked in the retail industry. Immediately a small business owner identifies the most targeted entrance an attacker is prone to target. Answering questions regarding the location of devices helps lead to identifying cost of equipment. Is this a mobile retail shop, stationary shop, public or private organization? Is just a terminal involved, or is a server on location? Identifying assets will be vital to the next method of identifying where data is stored.

In Table 6 the most common assets attacked for the past three years in each industry are grouped together. According to investigation of breaches conducted by Verizon and their partners three targeted assets are most common to be breached in each industry, servers, user devices, and a person (i.e. Phishing). Servers are the most targeted device common to threat actions. This poses a concern for majority of organizations who either store data on location servers or in cloud servers. Our next step will concentrate more on what's stored on servers and the cost of losing it. For now, we are only concerned with the cost of replacing these assets, downtime, man hours, or having to seek third party assistance to help clean and restore assets. These costs will calculate SLE. Calculation details are discussed Chapter VI.

Table 6 Industries Top Three Common Asset Breached Per Year

Years	Accom. (72)	Education (61)	Finance (52)	Healthcare (62)	Information (51)	Manf. (31-32)	Public (92)	Retail (44-45)
2017 1st	Server	Server	Server	Server	Server	Server	User Device	Server
2017 2nd	User Device	Person	Person	Media	Person	User Device	Person	Kiosk/Terminal
2017 3rd	Person	User Device	User Device	Person	User Device	Server	Server	User Device
2018 1st	Server	Server	Server	Server	Server	Server	Server	Server
2018 2nd	User Device	Person	Kiosk/Terminal	Media	Person	Person	User Device	Kiosk/Terminal
2018 3rd	Person	User Device	Person	Person & User Device	User Device	User Device	Person	User Device & Media
2019 1st	Server	Server	Server	Server	Server	Server	Person	Server
2019 2nd	User Device	Person	Person	Person	Person	Person	User Device	Person
2019 3rd	Person	User Device	User Device	Media	User Device	User Device	Server	User Device

Note:

- Accommodation = Accom.
- Manufacturing = Manf.

Smaller organization will need to tailor information according to their business needs. To improperly evaluate the cost of assets may lead to under or over estimating, resulting in poor security controls planning. Executives and stakeholders should be presented with a realistic picture in order to determine operational budget decisions.

Method 2: Once the cost of organizations' assets is determined, the focus transitions to the data stored within the devices. Compromised data records are the costliest expenditure of any breach. The Exposure Rate (discussed in Chapter VI) will help determine more of SLE cost. Figure 4 displays the average cost per record from a global perspective. Tallying the cost of an organizations record loss quantifies how much a company is at risk if compromised data occur. For the past ten years the average global cost per record is approximately $156.60 per record. This the second SLE calculations organizations combine with Method 1. Consequences of data records exceed beyond just replacement of records. The organization becomes liable not only for the record, but for negative outcomes each individual record may cause personally, as a result from the breach. For example, stolen credit card records can cause users to replace a card. The average cost to replace a bank card is $5, however the organization must consider replacing every record holder's card. Therefore, $5 x 1,000 records yield $5,000. Cost can rise steep and quick once breach is made public.

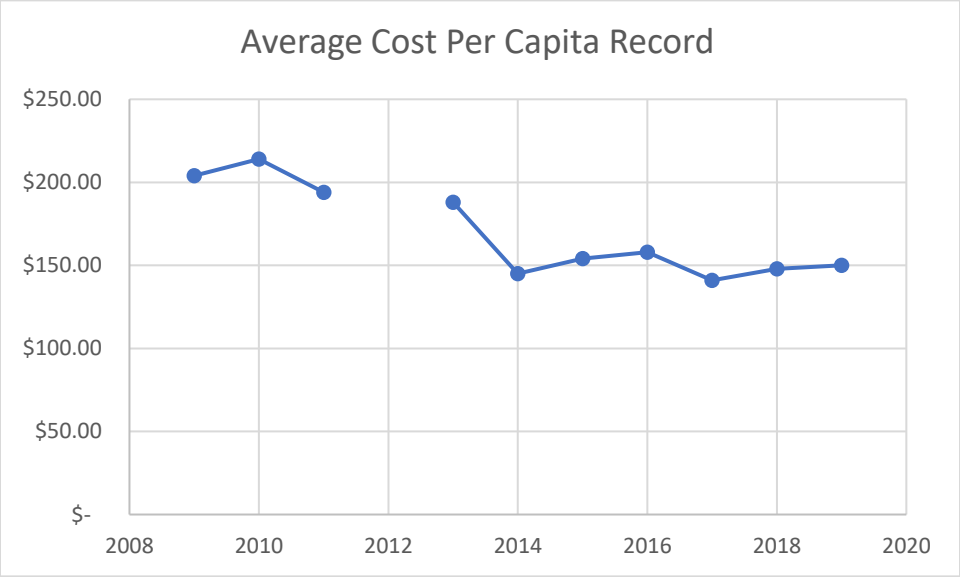

Figure 4 Average Cost Per Capita Record

Method 3: Direct and Indirect costs are additional expenses relating to loss or compromised data (details in Chapter VI). In addition to method 2 another Exposure Rate cost is added into the calculations.

Indirect costs include what organizations spend on additional resources to rectify a data breach. This could include man-hours consumed by distributing notification of the breach incident, investigation of the incident, notifying clients or customers, printing information and notices, etc. Also, included in these costs are loss of brand affect current and future cost, as well as reputation and customer turnover.

Direct costs include the cost an organization acquire to minimize the data breach and assist their victims. These costs may include forensic experts assisting in investigating a breach more in depth, hiring law firms to fight on behalf of the organization, protecting the identification of the clients or repairing damage incurred from the breach (i.e. credit repair). Figure 5 identify the direct and indirect global cost per capita for the past eleven years.

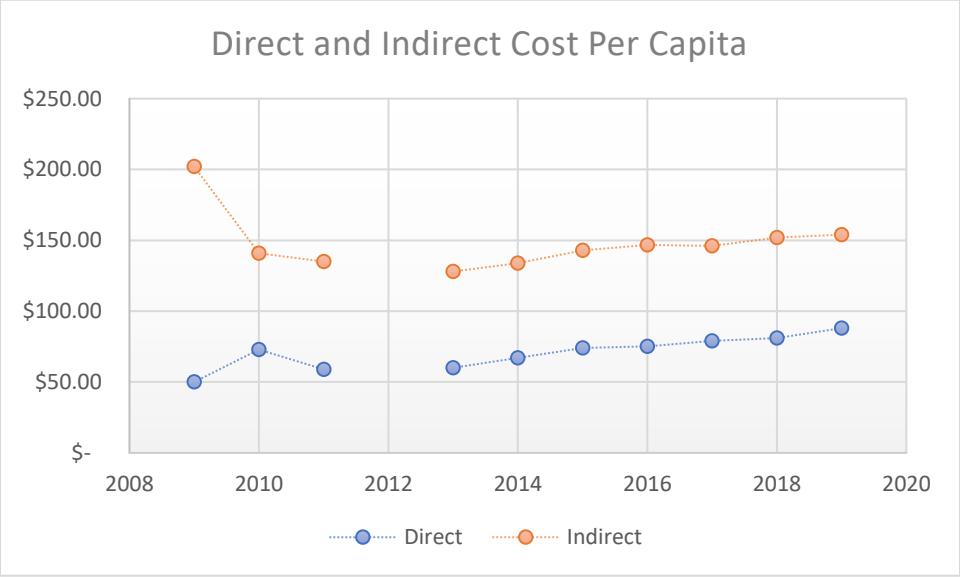

Figure 5 Direct and Indirect Cost Per Capita

Method 4: Customer turnover rate is calculated as a third factor of Exposure Rate. All industries are customer driven and comprised of serving clientele in some manner. When there is no demand for a service or product, an organization economic growth cannot sustain and resulting in greater loss of business, eventually closure.

Knowledge regarding customer trends over time help the organization understand a more in-depth picture of data breaches effect. Analyzing change over time highlights area of customer concern for industries. Figures 6-9 analyze customer turnover rate delivered from reports Ponemon Institute surveyed for the past three years.

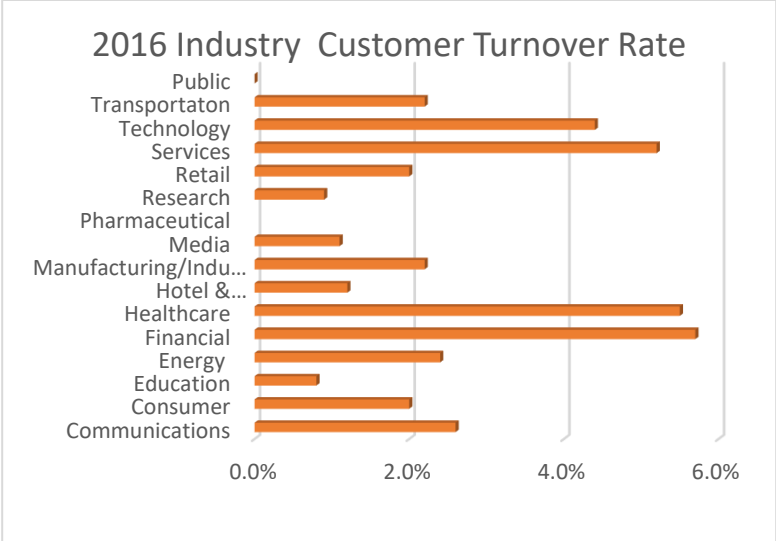

Figure 6 2016 Industry Customer Turnover Rate

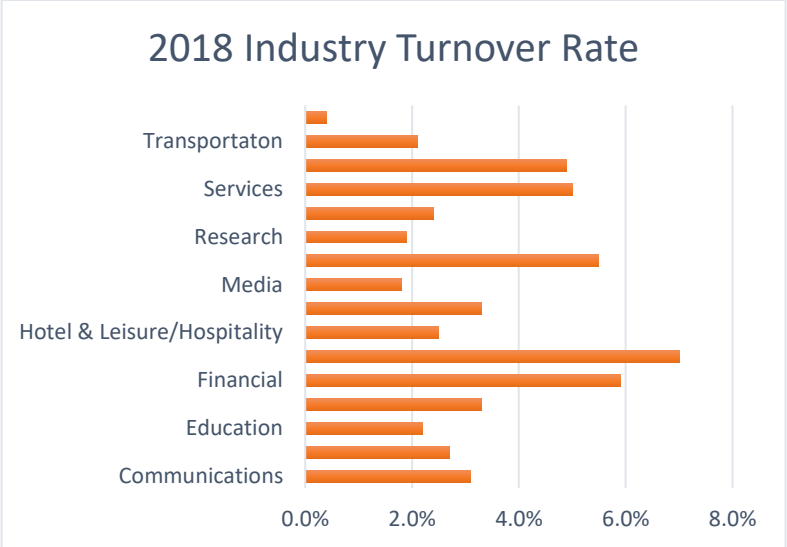

Figure 7 2018 Industry Customer Turnover Rate

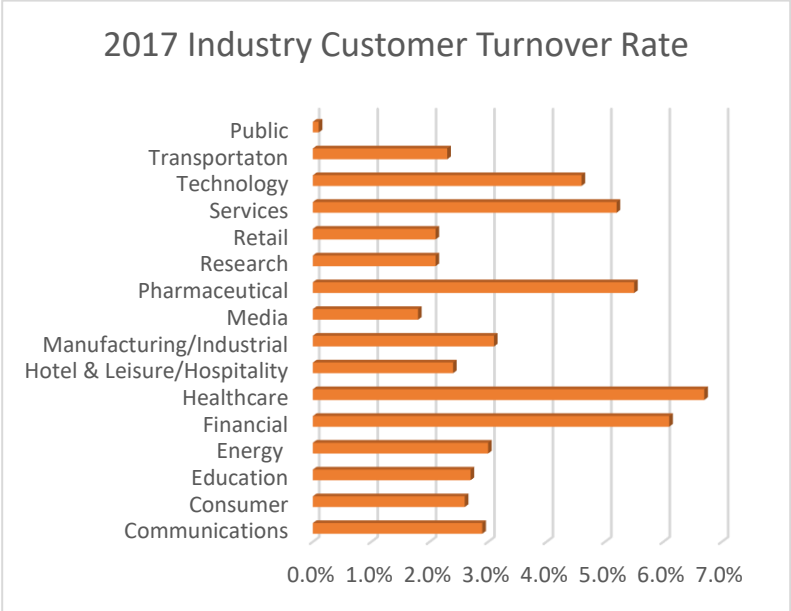

Figure 8 2017 Industry Customer Turnover Rate

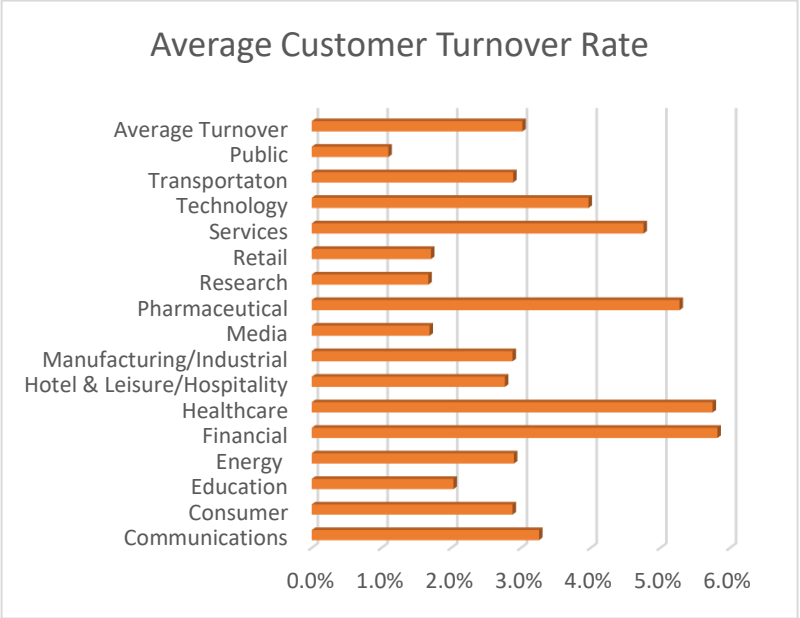

Figure 9 Average Customer Turnover Rate 2010-2018

Small and Medium organizations can estimate risk based on reports from Verizon and Ponemon. By recognizing patterns, threats, assets, and cost factors, management and executives are able to present solid foundational estimates for stakeholders to review and consider investing into operational budget to mitigate risk. Stakeholders need to see how investing will capitalize in the overall business plan. For risk budget to be effective, there must be a clear picture of the return on investment for the organization. The risk management plan must exemplify this return on investment will protect or mitigate the organization from failing to achieve its business plan from a catastrophic event. The framework in Chapter 6 will put the whole model together.

CHAPTER VI

CYBER RISK MANAGEMENT FRAMEWORK: AN INTEGRATION OF THE VERIZON AND PONEMON REPORTS

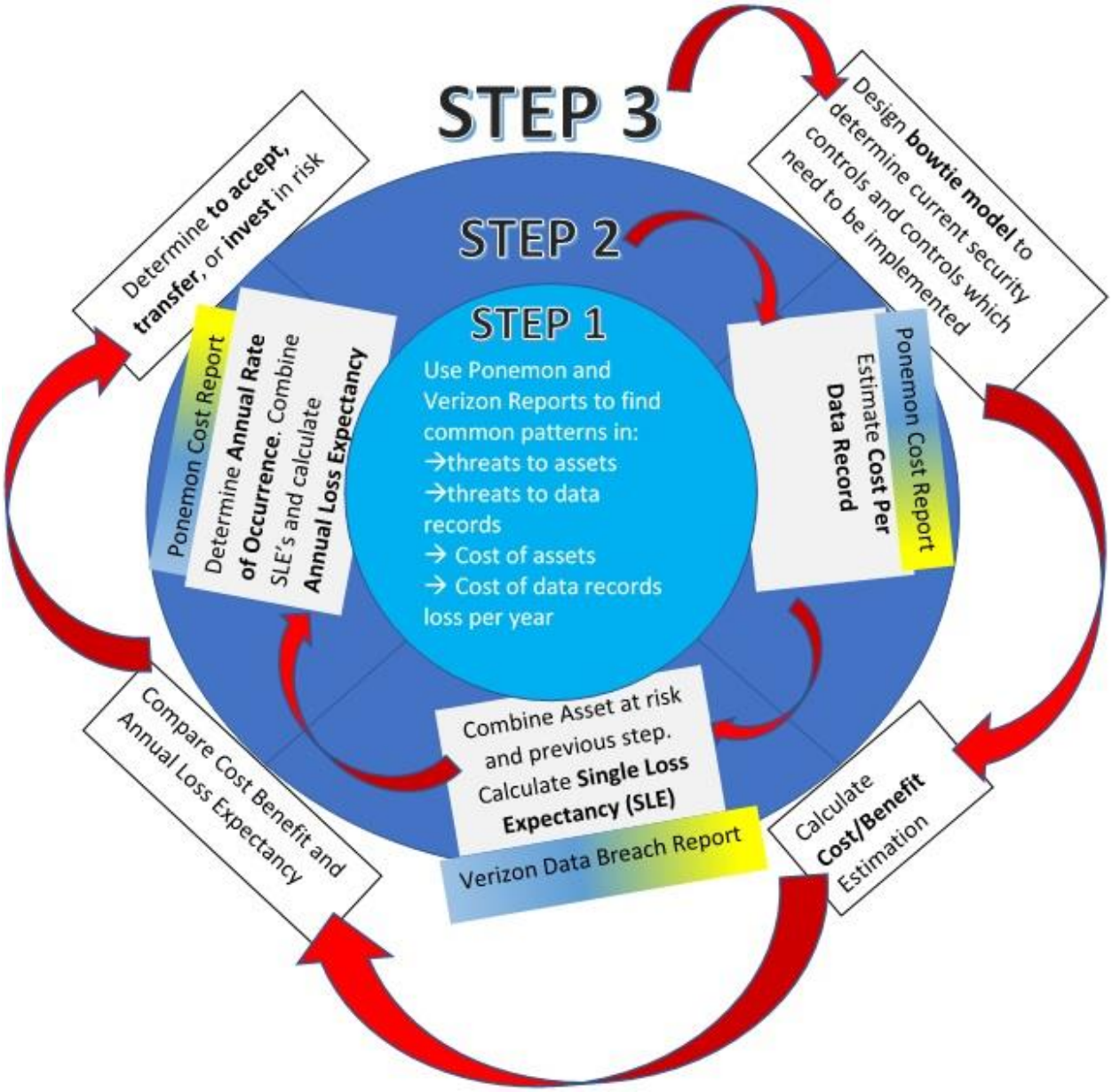

Figure 10 Cyber Risk Framework Model

The purpose of my Cyber Risk Management Framework is a strategy for small and medium (1,000 employees or less) organizations to identify, estimate, and prioritize risk to their organizational operation budget. What separates this framework is the integration of Verizon and Ponemon Data Reports to efficiently estimate cost of data breaches. The Bowtie Model has been introduced to precisely introduce security controls and calculate Cost Benefit Analysis (CBA). In efforts of making a Cyber Risk Management Framework more appealing to executives and stakeholders, this framework adopts language and methods from the FAIR Risk

Management cost effective approach. The four concepts below provide "common terminology" to assist in compressing the language gap between technical and executive staff members:

- **Cost-effective risk management**: a program that meets the definition of risk management; the combination of personnel, policies, processes and technologies that enable an organization to cost-effectively achieve and maintain an acceptable level of loss exposure.
- **Well-informed decisions:** every decision involves a choice
- **Meaningful measurements:** quantitative financial measurements
- **Accurate Models:** models of risk and of explicit risk management that can scale in real-life[xxxv]

The main goal of my framework is to provide a more cost-effective quantitative analysis approach to Cyber Risk Management. This purpose aligns with NIST guide to conducting a Risk Assessment which is to identify, estimate, and prioritize risk to organizational operation, organizational assets, individuals, other organizations, and the Nation, resulting from operation and use of information systems.[xxxvi]

Risk Framework is also an opportunity of sharing information not only with executives but with insurance carriers and other organizations. Risk Assessment Framework is a strategy for prioritizing and sharing information about the security risks to an information technology infrastructure.[xxxvii] As discussed in Chapter 2, insurance providers lack information and history of data breach cost. Therefore, premiums are higher and do not efficiently cover damages. Organizations with a framework in place identify areas of weakness, strength, and cost. Insurance carriers are more adapted to invest when operational risk management planning is justified.

The Cyber Risk Management Framework Model (CRMF) in Figure 10 is to be followed from an inner to outer approach. The inner core contains the reports used to gather necessary information to efficiently evaluate an organization completing step 2; identifying assets and estimating cost of loss to the organization due to a data breach. Organizing pre historical data will lead to an efficient risk quantification of assets and data records. The outer realm lead to determining

meaningful measurements of cost estimated benefits and calculating the total cost to manage cyber risk. Once completed executives will have a quantified cost-effective, well-informed decision risk analysis to present to stakeholders to invest budget for risk management in operational plan.

Stakeholders desire to see a more transparent, detailed, business applied approach to cyber risk management. Using Key Performance Indicators[xxxviii] to design my framework, there were ten recommendations which assisted in applying to stakeholder's appeal:

- Be based on quantities that can be influenced, or controlled by the user alone or in cooperation with others
- Be objective and not based on opinion
- Be derived from strategy and focus on improvement
- Be clearly defined and simple to understand
- Be relevant with an explicit purpose
- Be consistent (in that significance is maintained as time goes by)
- Be specific and relate to specific goals/targets
- Be precise – be exact about what is being measured
- Provide timely and accurate feedback
- Reflect the "business process"

Applying Quantitative Algorithm

The CRMF is designed from a three-step process: (1) Find common patterns, (2a) Determine Asset and its cost, (2b) Estimate data cost per asset, (2c) Calculate Data Cost, (3a) design Bowtie Model and calculate Cost Benefit Analysis, (3b) Determine Controls (3c) Calculate Cost Benefits and Rate of Return[xxxix].

These six steps reflect a combination of several resources including NIST Risk Management Framework, Cybersecurity Risk Framework, SANS Institute, and FAIR Basic Risk Assessment Methodology.

Step 1a: Find the Common Patterns

Tables 2 & 3 identify the nine most consistent common patterns used by attackers. With this information, small to medium organizations can identify significant assets targeted within your industry. Verizon Data Breach reports have investigated over 375,000 incidents, with over 17,000 involving data breaches as of 2018. Industries may retrieve these reports and discover which breaches affect their type of organization.

Step 2a: Determine Assets Value and Cost

Table 6 and Figure 4 connects targeted attacks in Step 1 to an asset and resource. Targeted assets are identified in Table 6 and Average cost of data records are estimated in Figure 4. Cost of records are subject to organization's size, data volume, location of equipment, and accessible copies (resilience).

Step two focuses on tangible and intangible resources. Tangible resources are considered to be physical and intangible resources include software, logical infrastructure, firmware or services. Evaluating these assets depend on two key factors, volume and value/liability.[xl]

The volume of assets allude to the fact of how many data records are in danger of being targeted by the same pattern of attacks. Simply speaking this is just the count of devices or systems with critical data records at risk of being compromised.

Asset value/liability are defined by three characteristics: criticality, cost, and sensitivity.

- Criticality of an asset considers the impact of an organization's productivity. If this asset were unable to perform how would revenue be affected?
- Cost of an asset relate to the replacement of a device or system. The amount of time it takes to not only replace, but restore the system to its full functionality.
- Sensitivity of an asset covers the unexpected consequences of an asset being compromised. To further collapse this point, four sub-categories can be considered:
    1. Reputation – the branding of the organization can be damaged or exposed to portray incompetence, criminal, or unethical management of protecting one's environment from danger.
    2. Competitor's Advantage – information exposed could enlighten competitors of sensitive, priority information.
    3. Legal – private, federal, and nonprofit lawsuits can be filed. Also, the organization can lose more revenue than expected in protecting client information or relationship
    4. General – indirect cost

Gathering and estimating the value of assets and data records will lead to more efficient calculations in Step 2. The value of data records will need to be tailored to the organization's environment. Reports from Ponemon and Verizon are based on a volume of records ranging from 1,000 to 99,000 records. Each organization will need to evaluate cost per record and base maximum cost value according to what Ponemon reports record.

Step 2b: Estimating Data Cost Per Record

Figure 4 yields an average amount of cost per record based on investigations over the past ten years. Cost per record for an organization is not expected to exceed beyond the global reports produced by Ponemon. One consideration may entail State or Federal laws enforcing additional penalties depending on location. In the U.S. each state is governed by their own State Laws. Forty-eight states now enforce regulations to govern data breaches, but there is no Federal Regulation, except best practices at this time. Therefore, each organization cost may differ

pertaining to their business needs. Once the total value of loss per record is determined, an estimation is established and calculated. For example, 2018 cost per record averaged $250. If my organization is a health clinic and I hold approximately 15,000 records of patients who have visited my clinic throughout the years, each record is multiplied by $250. Total loss is the product of 15,000 * $250 = $3,750,000. This would be considered the baseline cost for the total number of records. Security controls currently in place to mitigate attacks, are cogitated during cost/benefit calculations. Cost of Benefits are calculated after step 2c.

Step 2c: Calculate Data Cost

The goal of calculations is to determine the Annual Loss Expectancy (ALE) of each asset, including its data.

First, calculate the Single Loss Expectancy (SLE). Two calculations will be used to find the single loss expectancy for each asset, in addition to the data stored on the asset calculated previously in Step one. The Asset Value and Exposure Factor (EF) will determine the SLE dollar amount each threat potentially pose to an asset:

(Asset Value) * (Exposure Factor) = **SLE**

The EF represents the percentage of loss a threat has to a specific asset. To define percentages as a guiding point to the current example, take into consideration quarterly percentages, 25%, 50%, 75%, and 100%.

Example: A local dentist office wants to estimate the cost of a data breach occurring.

- value of a server is worth $10,000 (asset)
- Server contains approximately 5,000 records (asset)
- 25% of record loss has been discovered (EF)
- Cost of losing one record is estimated at $250 (based on Ponemon 2018 reports)
- Annual Rate of Occurrence once in ten years

SLE * Cost of each record = **Cost of Data Records**

(amount of records * EF) * cost of each record = **Cost of Data Records**

= (5,000 * 25%) * $250 = **$312,500**

Asset Value + Cost of Data Records = **Total SLE**

$10,000 + $312,500 = **$322,500**

Second, the Annual Rate of Occurrence (ARO)[2] must be considered to find the Annual Loss Expectancy (ALE):

Annual Rate of Occurrence represents the estimated frequency of a specific threat taking place within a year. Finding the product of this rate multiplied by the total SLE the Annual Loss Expectancy (ALE) is estimated. For this example, data breach is considered to only occur once in a year. There are instances when traces of attacks are left open through backdoor entrances and the attacker returns. Rarely within the same year. Therefore, ARO is 10% since this critical event is predicted to occur once in ten years.

[2]Annual Rate of Occurrence will need to be considered for each organization, and may vary. These rates will change the more data is collected in the future. Verizon Data Breach Reports, disclose popular attack methods annually for each industry. For instance, Table 3 identify nine attack patterns popular to industries each year. In Retail, only one Web Attack occurred in seven years. Therefore, a critical event which entails web attacks for an organization or business in retail, may not be as critical since its occurrence rate is once in seven years (14%).

SLE (total) * Annual Rate of Occurrence (ARO) = **ALE**

$322,500 * .1 = $**32,250** → If a data breach occurs only once in ten years

Calculating ALE will determine the financial cost of a breach. However, it is not the final cost presented to executive and stakeholders. Cost/benefit analysis must be taken into factor for meaningful measurements to be finalized. This will be discussed in Step 3. Also, the bowtie model in Step 3 will lead to identifying security controls in place. Stakeholders will make the final decision to reduce the cost of risk, decide which controls are worth implementing to mitigate risk, transfer risk to an insurer, or except the cost.

Step 3a: Design Bowtie Model

Once the bowtie model is completed, management and executives will have clear details regarding what security controls currently exist and what is necessary to implement in planning.

Designing the bowtie model reveal two important factors, causes and consequences affecting a critical event (top event) and barriers (security controls) to prevent or mitigate a critical event from occurring. Once barriers are placed within the model, the last model is finalized. The cost of a critical event can be assessed by estimating the cost of security controls in place and security controls necessary to implement. This is a decision executives and stakeholders can choose rather to embrace this cost or accept the cost of impact from a critical event. Figure 11 portrays a schematic of the bowtie model.

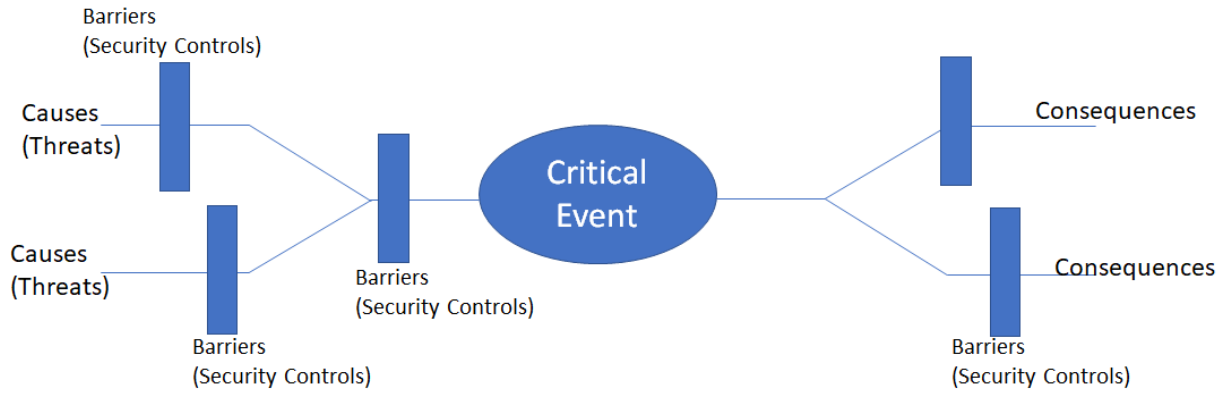

Figure 11 Bowtie Diagram

Cost Benefit Analysis (CBA) is determined by calculating the value of safeguards (security controls) to the company. The ALE before existing controls are applied must be subtracted from the ALE after controls are applied. This total amount will be reduced by the annual cost of each security control. Cost Benefit Analysis measures the benefits of a decision which is taking action minus the costs associated with taking that action:[xli] First calculate the value of safeguards to the company:

(ALE before implementing controls) – (ALE after existing controls are identified) - Annual cost of safeguard = **value of safeguard to the company**

Organizations are next to be taken into consideration, the benefits of implementing controls (barriers) and subtract the cost associated with taking that action. For the purpose of CRMF, the benefits of security controls are identified by protecting an organization from a critical event occurring. This amount will be subtracted from the ALE before and after existing controls are identified.

Security controls must be considered in its entirety when calculating the total cost. There are tangible, intangible, infrastructure, and man hour costs to consider:

- Product Costs (tangible)
- Design/planning Costs (man hours)
- Environmental Modification (individual organization infrastructure)
- Compatibility with other controls (individual organization infrastructure)
- Maintenance Requirements (tangible)
- Testing Requirements (tangible)
- Repair, replacement or update costs (tangible)
- Operating and Support Costs (man hours)

Once each control has been evaluated an accurate model can be completed.

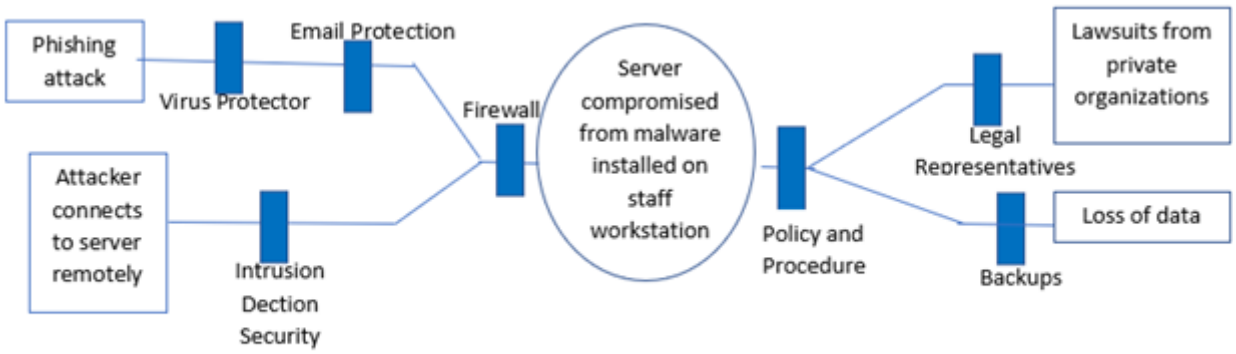

Figure 12 Bowtie Example

Step 3b: Determine Controls

Example Cont.: For the scenario described in Figure 12 example, concentration will primarily be on implementing only one security control. The local dentist office needs to know the cost/benefit of implementing a security control. They discovered from the bowtie model their current infrastructure only has an antivirus active on each computer which accesses their on-premises database. They would like to implement a firewall with Intrusion Detection Software (IDS) to filter traffic and protect the inside network.

- Existing Controls
  - Virus protection on 10 desktops = $600
  - Email protection through cloud services = $300
  - Server with access control = $500
  - Intrusion Prevention System = $1,000
  - Total Existing Controls Cost = **$2,400**
- Company decides to purchase a CISCO Firewall to implement control
  - Price of IDS firewall = $5000
  - Man - hours to configure 8 hours @ $250/hr.
  - Man - hours to install and test in network 8 hours @ $250/hr.
  - Licenses =$500
  - Security Certificate = $55 yr.
  - Possible downtime loss $2500
  - Total Control Cost **$12,055**

Step 3c: Calculate Cost Benefit and Rate of Return

(ALE before implementing controls) – (ALE after existing controls are identified) - Annual cost of safeguard = **value of safeguard to the company** (initial implementation)

($322,500 - $2,400) - $12,055 = **$308,045**

Value of safeguard / Single Loss Expectancy = **Rate of Return on Investment**

308,045 / 322,500 = **.955** or **96%**

Cost benefit of the dentist office implementing a firewall will benefit the company an estimated $308,045 to protect and mitigate the dentist office from a possible malware attack and compromising records on the server. For the initial $12,055 invested to implement a firewall in lieu of a breach occurring, the organization yield a 96% return on investment if the firewall stops the breach from reaching its server and compromising records. When configured properly the firewall will keep outside traffic from entering the network and attaining remote access.

The ALE if a breach were to occur is estimated $322,500. This example considered 5,000 records compromised by a malware attack. Assuming only 25% of records were compromised cost has been reduced significantly. Most breaches are not caught in time to limit the attackers damage. Data breaches are discovered after months of existing in the network 60% of the time.[xlii]

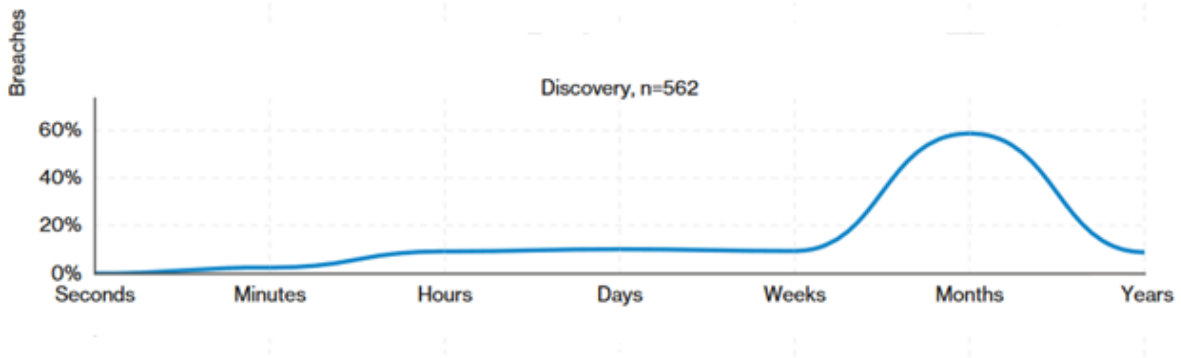

Figure 13 Discovery of Breach Timeline

This example has been simplified to identify only one critical event and a limited number of controls. For an organization this process may be repeated a number of times to account for all assets and records. For smaller organizations, at minimum the main asset which store data records is highly recommended to consider

CHAPTER VII

CONCLUSION

Quantitative analysis provides a financial scope to best manage a data breach occurring. With a base and implicit framework in place, managers and executives are able to have a jumpstart in organizing and presenting necessary details for stakeholders to invest and budget in operational plans. Cyber risk management cannot continue to be a reactive approach, as cyber breaches have proven to be the cause of organizations closing doors due to financial anguish. There must be a solid approach to attacking this catastrophic behavior before the action transpire and cause irreversible damage.

With the ability to track patterns, forecast estimations, and define a clear picture of current and necessary perimeters to mitigate catastrophic behaviors, organizations are better equipped to overcome the damage. A Quantitative Framework will deliver a guide to this proactive approach especially in small to medium organizations.

The CRMF entails necessary pre-historic resources to gather information regarding patterns of attacks and cost of breaches from dedicated reports by Verizon and Ponemon Institute. The reports unveil cost estimations for assets and data records, to calculate the SLE, ARO, and ALE based on the estimates pertaining to the organization. Next design a bowtie model to clearly define critical events susceptible to your industry/organization. Threats, vulnerabilities, consequences, and security controls must be clearly defined. Once Bowtie Model has been designed estimate the cost of two outcomes, current security controls in place and security controls necessary to implement. For each outcome calculate estimations. The final calculation combines all cost estimations and generate a cost/benefit estimation to observe return on investment.

Once return on investment is captured, executive managers can now present before the board and discuss the financial estimates of mitigating cyber risk. Stakeholders are presented with two important costs to determine the organization's future. The expected loss of business due to a cyber breach and the return on investment to prevent or mitigate a cyber data breach. Managing risk concludes in three decisions stemming from the quantitative framework provided, accept risk, transfer risk, or invest in risk.

REFERENCES

[i] NIST 800-137 p.423, FIPS SP 200 Adapted

[ii] NIST 800-137 p.424, FIPS 200 Adapted

[iii] MD Shahabuddin, 2018, Cybersecurity Challenges for Small Businesses

[iv] MD Shahabuddin, 2018, Cybersecurity Challenges for Small Businesses

[v] Marvell, "Risk Management Need to Start going Executives What they Want", https://acuitys3.s3.eu-west-2.amazonaws.com/s3fs-public/risk_management_needs_to_start_giving_executives_what_the_want_0_0.pdf

[vi] Veltsos, December 27,2017, Long Road Ahead or Unbridgeable Chasm? Lessons From the EY 'Global Information Security Survey', https://securityintelligence.com/long-road-ahead-or-unbridgeable-chasm-lessons-from-the-ey-global-information-security-survey/

[vii] Toregas, Zahn, January 7, 2014 Insurance for Cyber Attacks: The Issue of Setting Premiums in Context Report GW-CSPRI-2014-1

[viii] Insurance Journal, May 2018, "U.S. Cyber Market Grew 32% in 2017 But Most Small-Medium Firms Opted Out: A.M. Best", https://www.insurancejournal.com/news/national/2018/05/21/489930.htm

[ix] "How can we Improve Cyber Risk Management? (Business-driven security bridges the gap between cyber security and risk management)", https://www.rsa.com/en-us

[x] Mathieu Chevalier, July 5 2018, Small and Midsize Business Need to Focus on Cybersecurity

[xi] Biener, Eling, Wirfs, Insurability of Cyber Risk: An Empirical Analyst", The Geneva Papers 2015,40, (131-158), www.genevaassociation.org

[xii] Hoffman, Kannry, Levite, November 2018 Addressing the Private Sector Cybersecurity Predicament: The Indispensable Role of Insurance

[xiii] Harvey Nash, KMPG, CIO Survey 2018 https://www.harveynash.com/usa/news-and-insights/US_CIO_survey_2018.pdf p.44

[xiv] A. Ekelhart, S. Fenz, and T. Neubauer. Aurum: A framework for information security risk management. In System Sciences, 2009. HICSS '09. 42nd Hawaii International Conference on, pages 1–10, 2009

[xv] Rettas, Morishita, February 2019, "Implementing a Risk-Based Cyber Security Framework", www.cshub.com

[xvi] Townsend, November 13, 2018 State vs. Federal Privacy Laws: The Battle for Consumer Data Protection

[xvii] Hoffman, Levite, November 2017, "Private Sector Cyber Defense"

[xviii] Women Corporate Directors, 2018, "Cyber Risk Management Response and Recovery, https://www.mmc.com/content/dam/mmc-web/Global-Risk-Center/Files/WCD-MMC-Cyber-Risk-Management.pdf

[xix] Roy, January 2018, "Cybersecurity Professionals: Lack of Training Leaves Skills Behind", https://searchcompliance.techtarget.com/feature/Cybersecurity-professionals-Lack-of-training-leaves-skills-behind

[xx] Miller, April 2018, "Hiring and Training Challenges for CISO's in 2018", https://www.securitymagazine.com/articles/88891-hiring-and-training-challenges-for-cisos-in-2018

[xxi] CGMA, June 2013, "Activity-based costing (ABC)", https://www.cgma.org/resources/tools/essential-tools/activity-based-costing.html

[xxii] Ponemon Institute, IBM Security, 2019, "Cost of a Data Breach Report

[xxiii] Ruijter, Guldenmund, March 2016, "The Bowtie Method: A Review"

[xxiv] IADC, 2010, "Health Safety and Environment Case Guidelines for Mobile Offshore Drilling" Units. Tech. Rep. International Association of Drilling Contractors, Houston

[xxv] ISO, 2000, Iso 17776 – Petroleum and Natural Gas Industries – Offshore Production Installations – Guidelines on Tools and Techniques for Hazard Identification and Risk Assessment Reference Number

[xxvi] Sklet, S., 2006, Safety barriers: definition, classification, and performance.", p. 494-506

[xxvii] de Dianous, V., Fiévez, C., 2006. "Aramis Project: a more explicit demonstration of risk control through the use of bow-tie diagrams and the evaluation of safety barrier performance", p. 220-233

[xxviii] Margaret Rouse, Ben Cole, 2016, "OPSEC (Operational Security)", https://searchcompliance.techtarget.com/definition/OPSEC-operational-security

[xxix] Verizon, 2013, "2013 Data Breach Investigations Report"

[xxx] Verizon, 2014, "2014 Data Breach Investigations Report", p.15

[xxxi] NAICS Association, https://www.naics.com/search/

[xxxii] NIST Institute of Standards and Technology, April 16, 2018, Framework for Improving Critical Infrastructure Cybersecurity Vol.1.1

[xxxiii] Ponemon Institute, LLC, January 2010, 2009 Annual Study: U.S. Cost of a Data Breach p. 10-11,36

[xxxiv] Ponemon Institute, March 2012, 2011 Cost of a Data Breach Study: United States, p. 21

[xxxv] FAIR Institute, FAIR Risk Management, https://www.fairinstitute.org/fair-risk-management

[xxxvi] NIST, September 2012, "Guide for Conducting Risk Assessments, Special Publication 800-30, p. 98

[xxxvii] Rouse, October 2010, Definition "Risk Assessment Framework", https://searchcio.techtarget.com/definition/risk-assessment-framework-RAF

[xxxviii] Klipfolio, "What is KPI", https://www.klipfolio.com/resources/articles/what-is-a-key-performance-indicator

[xxxix] Tan, December 2002 "Quantitative Risk Analysis Step-By-Step"

[xl] The Open Group, January 2009, "Risk Taxonomy" p. 18

[xli] Kenton, June 23, 2019, "Cost-Benefit-Analysis", https://www.investopedia.com/terms/c/cost-benefitanalysis.asp

[xlii] Verizon, 2018, Verizon Data Breach Incident Reports, p. 10