2020

# Quantitative Risk Analysis for Improved Cybersecurity Risk Management

Project initiation: April 3, 2019

End date: Oct. 9, 2019

*Cybersecurity Category*

**Nomination submitted by**

NELSON P. MOE<br>
Chief Information Officer of the Commonwealth<br>
Virginia Information Technologies Agency<br>
July 15, 2020

# Quantitative Risk Analysis for Improved Cybersecurity Risk Management

## Executive Summary

The quantification of risk is a familiar activity to insurance interests, but no longer exclusive to that industry. Governments now are using quantification tools and analyses as part of business and/or risk management programs, particularly for financial management. In an era of widespread and potentially damaging cyber crime, cyber risk has emerged as an important budgetary concern for state government.

The Virginia Information Technologies Agency (VITA) in the Commonwealth of Virginia (COV) is responsible for digital government services for 65 state agencies, their 55,000 employees and 8.6 million end user customers. Virginia is one of the few states with an enterprise IT infrastructure and the resulting single cybersecurity overview. However, despite this agile view, when asked to predict costs for a potential cyber incident, Commonwealth planners were left wanting. High/medium/low risk was the only standard; there was no dollar figure attached to any applicable risk model.

Upon realizing this important gap amidst the rise in dangerous cyber activity, Virginia's Secretary of Administration challenged her Chief Information Security Officer (CISO) to create and develop an accurate and defendable methodology to fill the gap. This work had not been done before at the state level, but its challenges were clear.

The chief and immediate goal was to standardize and create predictable cost models for agency consumption. Project scope included estimation of costs associated with detection, and response and recovery activities of various cybersecurity incidents. Stakeholders include financial planners at the executive branch, independent agencies and institutions of higher education - and thus, Virginia's residents and end users.

The Quantitative Risk Analysis project, one of the first of its kind among states in the country, sought to define and standardize the actual cost of a cybersecurity incident, and most importantly, assign real dollar values. A companion risk analysis focused on tools to mitigate or address cybersecurity risks, and what the cost of those tools would and should be.

This project's ultimate benefit is to better protect Virginia's IT systems, government institutions and members of the public by allowing prioritization of investment where it is most needed. It now aids Virginia agencies in more accurate financial and risk forecasting of potential cyber events. Virginia's model is now also available to any government wishing to better predict and value cyber risk, in pursuit of shared cybersecurity goals.

## Concept

VITA, its Commonwealth Security and Risk Management (CSRM) division, and its CISO are responsible for IT security and risk management for executive branch agencies. Scope includes protection of computer systems and networks from theft of or damage to hardware, software or electronic data, as well as from the disruption or misdirection of the services they provide.

Virginia's Secretary of Administration challenged the CISO to provide quantifiable data on risks involved, recognizing limited resources and a recent surge in ransomware attacks across the country. While trying to budget, she determined that the industry ranking of red, yellow and green (or high, medium and low) were unable to inform the necessary financial data she needed to quantify the devastating repercussions a data breach could be for an agency. It became glaringly evident that executive leadership needed an enhanced ability to make informed risk-based decisions in the following areas:

- IT investments
- Security enhancements
- Acceptance of cybersecurity risk
- The need for cyber liability insurance
- Protection of AAA bond rating
- Understanding of reputational risks

Properly identifying and forecasting associated costs are paramount. Data breaches result in both direct costs of resolving the breach and the indirect costs of time, effort, loss of productivity and other organizational resources. To best address both types of costs, four broad cost drivers and associated activities were identified by Virginia's risk management team:

- **Detection and escalation** - Activities to detect and report a breach (forensic and investigative actions), including emails, letters, outbound telephone calls, or general notice to data subjects that their personal information was lost or stolen; communication with regulators, determination of all regulatory requirements and engagement of outside experts
- **Notification costs -** Activities include the notification of individuals who have had data compromised in the breach (data subjects), including: setting up helpdesk activities, robust communications channels, credit report monitoring, identity protection services, issuing new accounts and legal expenditures
- **Post-data breach response –** Activities include setting up processes to help individuals or customers affected by the breach, including: administering a helpdesk, report monitoring, identity protection services, and addressing legal expenditures and potential fines
- **Lost business cost -** Activities include addressing customer turnover, business disruption, system downtime, loss of reputation and diminished goodwill.

To deliver needed tools to accurately cost this activity, Virginia's risk management team first investigated the Factor Analysis of Information Risk (FAIR) model, an international standard quantitative model for information security and operational risk. The team determined that while it was a good method, it would require too much time to analyze risk on a case-by-case basis and would not be financially feasible.

Next, the team reviewed and chose as its baseline the work of Larry Ponemon and his annual data breach reports. The cyber industry does not have a standard cost measure for a data breach, but Ponemom is credited for one of the more accurate cost-per-record methods. It takes the size of the breach, systems used and number of records, and calculates costs of penalties, notifications and lost revenue for recovery.

CSRM next needed to customize the model for government. The team quickly determined the cost-per-incident record was the first place to start. Most data breach cost calculations include a linear increase in cost. These models include a total breach cost that continually increases per record without ever reaching a cap. Within the Commonwealth, the model showed that once a data breach reached a certain size, costs did not continue to increase at a consistent rate. The output showed the total costs increasing at a slower rate as the number of records increased past a certain point. After evaluating the model, CSRM determined calculating the cost per record loses its accuracy at the extremes. The team was able to take the resulting model and test it using the data collected within the enterprise security and risk governance management system.

This project benefited significantly from CSRM and agencies' ongoing work to build out the Commonwealth's enterprise security and risk governance management system, Archer. This system has been used to collect and analyze data over the last five years about agency risks, security incidents, application information, and several other technology items. Each agency's information technology resource (AITR) annually certifies its agency's data and applications in Archer to ensure the system accurately represents each agency's business and corresponding risk inputs.

Organization size was identified as a valuable risk variable. Larger organizations have made significant investments in cybersecurity, and tend to have more security controls resulting in a lower likelihood of a cyber event. Government cyberattack victims are typically small- to mid-sized agencies who struggle to spread budget sources to cover all aspects of cybersecurity.

VITA's security architects review entries in Archer and determine residual risk for missing controls. This analysis helps determine if the likelihood of a security breach will cost more to figure out what happened (who, what, why) than the controls to make the security fix.

For example, if it costs $20,000 to fix a $180,000 risk, then the architect would recommend that the agency make the fix. It is not in the best interest of the Commonwealth to carry that much risk for a proportionally small price tag to fix the security control.

In order to identify the Commonwealth's potential amount of risk, a framework has been implemented to find control weaknesses. Every year, Commonwealth security requires service providers to complete a control audit by a third party. Every three years, agencies are required to complete a risk assessment, business impact analysis and audit. Archer correlates the resulting data and determines the baseline and residual risk based on missing controls, the value of data on the system and the impact to agency business. In addition, the Commonwealth catalogs the controls agencies have the most difficulty implementing and performs risk evaluations to determine the residual risk.

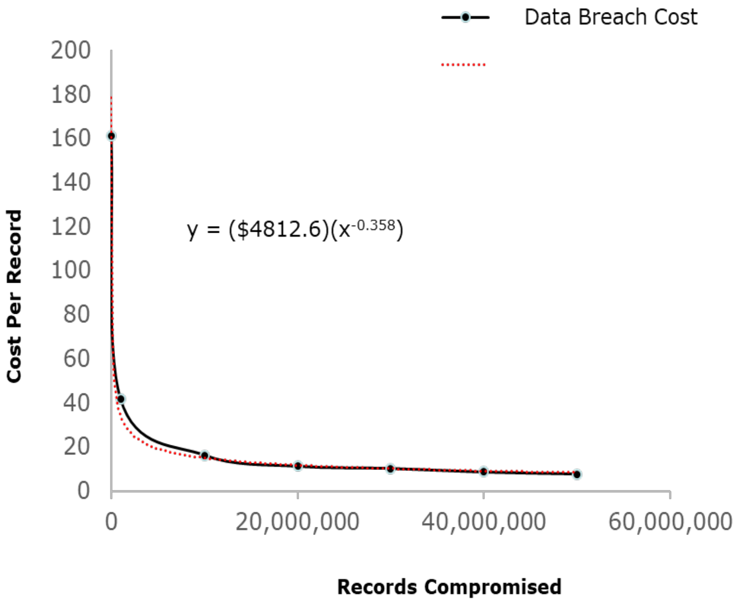
For example: an agency submits a template on a specific application (A) that identifies a security control that is NOT in place. This control is then tied to a vulnerability in the system, e.g., personal identifiable information records. The formula (quantitative risk analysis), created by VITA's risk team, which is already loaded into the Archer system, runs on application A and tells the team how much insurance is recommended.

VITA recognized needed refinements in key areas to begin quantification of systemic cyber risk:

- The calculations identifying the likelihood of an event
- Representation of the reputation risk due to a compromise
- Risks due to third-party hosted environments must be represented
- Dashboards and reporting at the system, agency and Commonwealth level showing the amount of risk the Commonwealth holds

VITA's risk management team created a formula with applied data, leveraged with Larry Ponemon's equation, and entered the data into their risk management system. The system is able to calculate the information on the fly and present agencies with the amount of risk they are currently experiencing based on the configuration of their environment. A graph was created to help visually represent the risk calculation formula. The Commonwealth calculates the risk components using the following:

- Inherent risk = $ per record x record #
- Residual risk = inherent risk x annualized loss expectancy of a system of that size
- Total residual risk = residual risk + ((sum of identified controls not in place / total identified controls) x residual risk)
    - 5 controls missing ~ 4% increase from baseline annual loss expectancy of a system that size
    - $100 annual loss expectancy becomes $104



Use case example: Agency XYZ wants to procure a cloud service. The agency estimates that the application will store 75,000 health records. The vendor has agreed to include $5,000,000 in cyber liability insurance. Is this amount enough?

- Number of records: 75,000
- Baseline risk:
    - Industry standard: $6,488,871
    - COV: $2,162,957
        - Cost per record= ($4812.6)($x^{-0.358}$)
        - x = Number of records (75,000)
        - Estimated baseline risk = ($4812.6)($75000^{-0.358}$)(75000) * 1/3 = $2,162,957
- Controls missing modifier: 30%
    - Missing controls increase the risk
    - Controls are weighted by impact

    Residual risk/data breach cost estimate: $2,811,844

    Use case conclusion: utilizing its risk model, CSRM concluded that $5,000,000 of cyber liability insurance should be adequate to minimize risk to the Commonwealth.

Example: South Carolina data breach in 2012

- Assumed all citizens of South Carolina were impacted by the breach
- Breach impacted Dept. of Revenue systems

- Number of records: 5.7 million
- Estimated breach costs: $20 million
    - Adjusted breach cost for 2019: $30 million
- Baseline risk
    - Industry standard: $104,628,843
    - COV: $34,876,281
- Controls missing modifier: 16%
- Residual risk
    - COV: $40,456,486

## Significance

As a result of this new model, executive leadership has an enhanced ability to make informed risk-based decisions in the following areas:

- IT investments
- Security enhancements
- Security exceptions
- Cyber liability insurance
- Protection of AAA bond rating
- Understanding of the reputational risks

This project reflects close alignment with NASCIO's first priority for 2019: cybersecurity and risk management. It also contributes significantly to several other national and state priorities including budget, cost control and fiscal management plus data analytics and management. As one of the first states in the nation to undertake the task, Virginia's efforts continue to pioneer innovation and embody industry goals of transformation through technology.

The project aligns with the budget, data and cyber goals of two gubernatorial administrations, supported legislatively by funding for staff and implementation. It promotes closer collaboration among VITA and agencies on cyber protection, and provides added benefits of improved financial security for participants.

The project also furthered cybersecurity work done by VITA and agencies in compliance with a previous administration's Executive Order 6  which required inventory of agency data and applications. This existing data set collection enabled CSRM to quantify risk quickly, once the formula had been completed. An unforeseen return on investment has been achieved for VITA's enterprise governance, risk and compliance tool Archer (2013). The tool has been key in applying and sharing risk information.

VITA used the Center for Internet Security's (CIS) top 20 critical controls as a starting point for this effort. The CIS controls are mapped in Archer using the National Institute of Science and Technology (NIST) Framework. Additional controls will be added over time as they are evaluated.

VITA promotes the awareness and education of this tool with agencies through monthly Information Security Officer Advisory Group (ISOAG) meetings. The meetings bring the information security officers together regularly to reinforce security concepts and explain how their data influences risk measurements within the Commonwealth.

VITA is empowering agency information security officers (ISO) to use the tool to enable agency leadership to make better and faster decisions in securing their IT landscapes.

## Impact

VITA’s security team now has a standard against which to review agency risk acceptance requests and determine the impact of approvals. The team can rank the baseline risk and compare it to the cost of insurance in circumstances when a security control is not in place.

New model component definitions now guide risk management for agencies:

- Baseline risk: risk incurred for agencies with basic cyber hygiene program; each application measured for likelihood of breach and impact of breach
- Residual risk: risk incurred by the Commonwealth after identifying missing security controls; missing controls increase the likelihood of a breach
- Data breach cost estimate: based on industry trends and Commonwealth costs; formula is based on line of best fit for data collected

Agencies already benefit from Archer’s data collection, and can monitor and use these metrics to further scale benefits and cybersecurity costs.

CSRM is now using this model in collaboration with the Virginia Department of Treasury to aid in its effort to procure umbrella cyber liability insurance for the Commonwealth.

The model implemented provides cost savings benefits, as well. Applying this methodology to the environment, including where risk was already transferred, VITA was able to reduce the cost per record by two-thirds of what the Ponemon Institute reports.

The CIS has noted that few states could have done quantifiable risk analysis like the Commonwealth, since they did not have the needed data available. Virginia, being a centralized IT shop, was able to create and utilize the formula for the Commonwealth.

A cornerstone of CSRM’s risk management is to ensure Virginia and its agencies are making good investments in cyber enhancements. By developing a quantitative risk analysis equation to attach a dollar sign to the cyber liability insurance and limit the Commonwealth’s cyber risk exposure, the team has transformed the landscape of cybersecurity in Virginia.