X-Analytics: The Origin Story

31
JUL 2018

Recent Posts

GDPR may be all the rage, but what's really important?
May 23, 2018

Study Findings: Inadequate Cyber Risk Measurement to Sustain the Cyber Insurance Market
April 24, 2018

Inconceivable! A Common Language for Cyber Risk
March 20, 2018

A New Era: Cyber Risk is Business Risk
February 27, 2018

2018 Predictions: A New Era of Security or More of the Same?
January 16, 2018

By Robert Vescio, Inventor of X-Analytics and Chief Analytics Officer at SSIC

When It Comes to Measuring Cyber Risk, Financial Impact is The Key

Over the course of my 20+ year career, I have learned how to quickly spot what does and doesn't work in the realm of cybersecurity risk. As we all know, there are a variety of risk management methods being used independently and in combination. Some are well respected, some are overly used, and some are inherently flawed. Of course, use and popularity of the method doesn't matter if this one simple question can't be answered:

Is this cyber risk method based on objectivity or nonsense? In other words, is the method a case of "garbage in, garbage out?"

Further, "Does the method help me forecast and evaluate an organization's financial risk together with the identification of procedures to avoid or minimize impact?"

Some of you may be wondering why I'm stressing financial risk under the context of cyber risk. Well, that is because cyber risk (in its own context) doesn't really matter to anyone outside of the technology or security groups if it doesn't have financial relevance. Additionally, all adverse cyber conditions (based on malice or error) have a financial consequence, such as the cost to remediate, lost revenue, and protracted damages. The understanding of financial consequences should be the basis for all cyber risk remediation, transfer, and acceptance decisions.

For most of my career, I have been using the questions above to determine the quality of the many risk management methods that I was asked or expected to use. Even though I never came across a method that truly satisfied both questions, I did come across several that could partially answer the question. Below are just a few of the methods commonly used to "measure" cyber risk:

- **The Smartest Person in the Room Method**: This is the method in which someone's opinion, intuition, or desire decides drives all decisions. This method lacks structure and relies solely on a gut feel. It is not rooted in structure, mathematics, objective data, or anything else that can be measured over time. By its very nature, it doesn't lead to the ability to forecast and evaluate an organization's financial risk.
- **The Compliance Method**: This method is based on a group of collective minds that ultimately leads to some sort of compliance framework or checklist. Even though the framework or checklist provides structure and the ability of measurement, it is rooted in a collective opinion, not objective data. The compliance method sets an expectation that all organizations are the same and that the compliance framework will reduce risk equally across all organizations, which is clearly not true. This method lacks the ability to forecast and evaluate an organization's financial risk and the ability to objectively prioritize procedures to minimize risk.
- **The Heat Map Method**: This is a method that attempts to incorporate structure, mathematics, and objective data with regards to cyber risk management. It provides an understanding of two things intersecting, such as threat and impact or vulnerability and criticality. The use of numerical or verbal scales along with color codes are used to illustrate which things are good, bad, and ugly. It is assumed, by many, that this method is better than the two other methods I listed above. However, there are problems with this method. First, many of the scoring methods are not based on extensive research (or data science). Second, most of the heatmaps are based on two dimensions, and risk is generally based on the combination of three dimensions (Threat * Cost * Vulnerability). Third, the methodology ignores the possibility of uncertainty. And fourth, heat maps lack a means to forecast and evaluate an organization's financial risk, even though they do produce (even if false) a means to prioritize procedures to minimize risk.
- **The Value at Risk Method**: This is a method that attempts to incorporate structure and complex mathematics to produce quantitative risk management outputs, which could also include the forecast of financial risk. In some circles, this is considered the best method since it uses sound mathematics. However, this method could be fundamentally worse than any of the above methods if the inputs are not objective and based on research. This method requires an organization to know how to decompose risk scenarios, has the ability to populate key variables without being

overconfident, and truly understands how much financial damage would be caused by a particular threat exploiting a particular vulnerability within a known asset. Most value at risk methods would be equivalent to giving a meteorologist a weather model without 100 years of historical data when in fact, it is the 100 years of data that make the model relevant.

As you can see, all of the above methods have problems and some have benefits. None of them were able to answer both of my questions. This presented both an opportunity and challenge. What if I could create a method that was objective, could help me forecast and evaluate an organization's cyber risk, and could identify procedures to avoid or minimize impact?

As I sought to answer this question, I witnessed an interesting market dynamic. The cybersecurity vendors were using fear and uncertainty to push their products as a promise of safety, while the insurance industry was beginning to roll out products that attempted to qualify or quantify risk exposure. While risk exposure (such as cyber event probability, impact, and expected loss) was extremely important to the insurance underwriting teams, most of the cybersecurity vendors had no desire to produce this type of output — with an ultimate fear that it would erode their market position. It became clear to me that two worlds—cybersecurity and insurance—were primed for a huge collision. I could see that a wholly new approach was needed to measure risk and bring clarity to both industries.

Inventing X-Analytics…

All of the above served as my basis for developing X-Analytics□. I set out to create an objective cyber risk measurement method and model that could bring clarity and reduce economic uncertainty. By design, X-Analytics had to be mathematically sound, rooted in unbiased research, and easy for someone to use. I spent a good six months experimenting with formulas, finding contrasting data sources, and collecting constructive feedback from peers and potential future customers. There were times when I had to throw out entire sections of the model and start over, discard what some consider to be great data sources (but were inherently flawed), and modify the look and feel of certain outputs.

Throughout the design phase, I was keenly focused on the pros and cons of each of the methods I listed above. I didn't want to entirely discount the knowledge that the cybersecurity and risk leaders have of their specific organizations, but also wanted to ensure that all of the backend variables were populated via objective data. To maintain quality and integrity, I used the following in my design process.

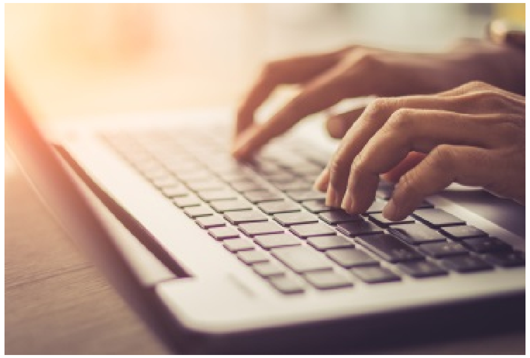
1. **Structure**: Without structure, I wouldn't be able to keep the numerous data sources organized. Instead of reinventing the wheel, I simply chose to adopt VERIS (see veriscommunity.net) as my underlying structure. The schema is easy to adopt and several of my intel sources are already in that format. Everything that is fed into my model, such as customer data, third party intel, and cybersecurity frameworks, align with this schema.
2. **Objective Data**: Let's face it, most people aren't calibrated and can't answer truly important questions that are necessary to quantify risk and associated economic outputs. As a result, the model combines numerous statistical and representative data sets to pre-populate backend variables that would essentially be impossible for most people to answer.
3. **Completeness**: Since most cybersecurity risk management methods and products fall short of telling the complete story, I wanted to be sure that my method was able to mathematically combine threat and control details to risk, risk to financial outputs (such as probability, impact, and expected loss, and financial details to prioritized guidance). In short, everything had to be connected in a meaningful way.
4. **Ease of Use**: My method had to be easy for anyone to use. Instead of asking the user to decompose risk scenarios and provide nonsense (or made up) inputs, I wanted to provide easy to follow inputs and easy to follow outputs around a predefined set of applicable risk scenarios that automatically map to a pre-defined set of cyber peril categories. Essentially, I needed to bring simplicity to a world that is already extremely difficult.

As things stand today, the model has been patented, gone through several successful validation exercises, and is used being used in a wide range of industries throughout the world. In the cyber insurance industry, X-Analytics is being used to modernize the cyber insurance underwriting process and how the industry overall expresses cyber risk exposure. X-Analytics is also being used to present cyber risk in economic terms to executives and boards of directors. Finally, it is transforming the way that certain markets conceptualize cyber risk management.

What is X-Analytics?

X-Analytics® is the world's first cyber risk quantification model used to financially model cyber risk exposure end-to-end across the risk management ecosystem. Our patented model is being used to underwrite billions of dollars of affirmative cyber risk insurance, produce board-level cyber risk analysis, and quantify aggregated cyber risk across portfolios.

DISCOVER MORE



BLOG See more »

NEWS See more »

EVENTS See more »

X-Analytics: The Origin Story

GDPR may be all the rage, but what's really important?

SSIC Advances Cyber Risk Analytics with New Release

Unisys Unveils TrustCheck™, the First Subscription-Based Service to Help Security Teams Continually Assess and Prioritize Cyber Risk in Economic Terms

Cyber Risk Insights Conference — New York

October 25, 2018

Contact us today

Global Headquarters
Washington DC
1501 Wilson Boulevard, Suite 1025
Arlington, VA 22209
info@securesystemscorp.com

ABOUT SSIC PRODUCTS AND SERVICES NEWS & EVENTS BLOG GLOBAL OFFICES

Let's connect

in

SSiC