protiviti®
Face the Future with Confidence

Moving Beyond the Heat Map: Making Better Decisions with Cyber Risk Quantification

A major cybersecurity event can dissolve millions of dollars in assets and tarnish even the strongest company's reputation. As cybersecurity concerns grow and evolve, companies need to be prepared for the inevitable cyber attacks with strong defenses to identify breaches and minimize damage. But how does leadership know where to invest in cybersecurity? How much is at risk? What should be prioritized?

Why are traditional cyber risk assessments failing us?

Our clients struggle with similar issues in their cyber risk programs. We see boards of directors pushing for cybersecurity risk reduction and asking if the existing cyber insurance policy has enough coverage due to near-miss cyber incidents. Chief information security officers (CISOs) are tasked with producing updates to the board despite being plagued with resource constraints. On top of that, the need to comply with various regulations has transformed the cyber risk assessment process into a plethora of checklists and gap assessments – in turn focusing the cyber risk program on controls rather than risk.

How can you answer the board's questions with traditional risk assessment methods?

- Do we have enough cyber insurance?
- Are we doing enough to minimize risk? How much would a breach cost us?
- Are we spending our cybersecurity budget on the right things? What is the ROI?
- How much risk do we have? Are we spending too much or too little?

Risk management, at its core, is a fundamental exercise in decision-making - but if you can't use the output of your assessment for risk decisions, what's the point?

Traditional Risk Assessment Methodologies

We see traditional risk assessment methodologies deployed for cybersecurity risk with the following objectives, approaches and results:

OBJECTIVE	APPROACH	RESULT
• Understand the cybersecurity risk to the organization • Fulfill regulatory obligations for risk assessment	• Rely on either top-down or bottom-up assessment • Multiple annual assessments to fulfill separate obligations • Stakeholders determine risk based on opinion of likelihood and impact	• Heat map or similar view of risk based on likelihood and impact • Generally, more qualitative than quantitative • Produces list of identified control gaps
Issues	**Issues**	**Issues**
• No clear definition of risk vs. threat vs. vulnerability • Subjective scoring – "I think that is a Low, not a Medium." • Without the ability to speak the same language, no one in the organization can measure risk or compare one risk/threat/asset to another • Cyber risk is spoken about differently than other business risks	• Series of competing frameworks (ISO, NIST, CSF, homegrown) • Deterministic model of risk (risk = likelihood * impact) that doesn't take into account probability of risk event • Allows stakeholders to "game the system" to get the rating they want • Organizational stakeholders assessed multiple times a year and asked a similar set of questions each time	• Results of each assessment seem to be different depending on who shows up for the meeting • Utilizes a "scoring model" - but that doesn't mean you can add or multiply the risk for a holistic view • Results are a laundry list of "gaps" with no prioritization • Given no one uses the assessment for decision-making, it has devolved into a check-the-box exercise

CISOs often take the information from a multitude of control gap assessments along with operational metrics and attempt to build dashboards to cover cyber risk. Yet, they still cannot answer the board's questions or know if they are spending too much or too little on cybersecurity.

What are forward-thinking companies doing to increase transparency on cybersecurity risks?

The good news is, there are better methodologies for cyber risk assessment that allow organizations to truly understand their cyber risk landscape and appropriately mitigate that risk. Quantitative models, such as Factor Analysis of Information Risk (FAIR), can be used to measure the financial impact of cyber risk and provide a standard risk language to ensure consistency. Using methods like FAIR, an analyst can demonstrate the risk reduction of a control in financial terms and evaluate potential investments in cybersecurity technology. Being able to demonstrate "return on control" the same way as for any other capital investment is a powerful tool for any organization.

How does cyber risk quantification work in practice?

Cyber risk quantification uses existing models and probabilistic simulation methods to more accurately describe the cyber risk facing an organization. These are not new models or techniques for risk management – but the application to cybersecurity risk is a newer concept. This kind of risk analysis involves the business users, asset owners and other people who may not have been previously included in cyber risk assessment. These are the people who are closest to the potentially threatened assets — the "crown jewels" — and who know the value of what needs to be protected from a business standpoint.

Cyber Risk Quantification Process

1 Identify Threat Scenarios

Determine the events that could result in harm to an asset and/or the organization

2 Gather Data

Hold discovery workshops to obtain objective and subjective data points on various threat scenarios

3 Model Data

Apply gathered data to probabilistic models to describe the cyber risk facing the organization

4 Quantify Risk

Assessment results provide a meaningful view on the magnitude of cyber risk facing an organization — serving as a powerful decision-making tool

Quantifying the risk starts with determining the different threat events that could result in harm to an asset and/or the organization, such as weather, geological events, malicious actors, errors and failures. These different threat scenarios are determined based on a review of external threat intelligence products and published breach data. Data on the likelihood and magnitude of these events at an organization, both objective and subjective, is collected through a series of discovery workshops organized by the cybersecurity function in which subject-matter experts are interviewed to understand how controls function to protect against a series of threat scenarios. Data comes from a diverse variety of sources, including review of existing and proposed policies and standards, interviews with subject-matter experts and control owners, and collection and review of objective data from system-generated reports, management reports and manually collected metrics.

The information gathered through various discovery exercises is modeled statistically so that Monte Carlo simulation can be used to quantify the cyber risk the organization faces based on the probable frequency and probable magnitude of each threat scenario. The results show risk plotted on a continuous curve showing the frequency and magnitude of threat events. Risk is quantified – organizations know, in monetary terms, how much is at risk and with what confidence.

We commonly find companies that struggle to adopt more mature cyber risk quantification approaches share one or more of the following misconceptions: cybersecurity is too complex to measure accurately, they don't have enough data or cyber risk quantification requires expensive tools.

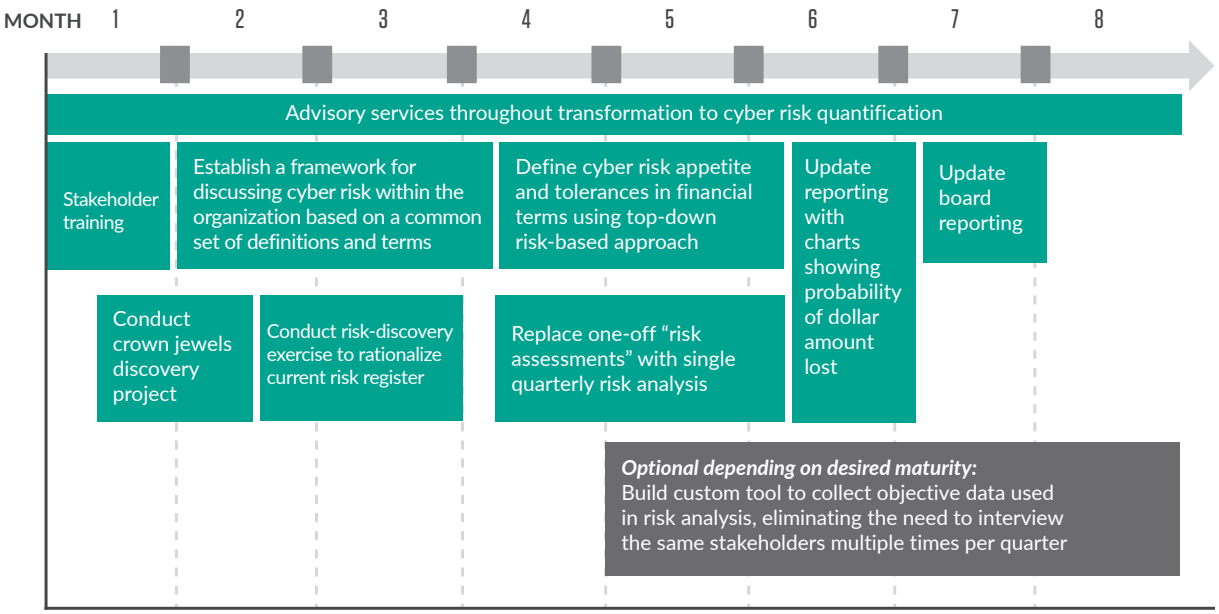
But as Douglas Hubbard, author of *How to Measure Anything in Cybersecurity Risk*, says, it's good to keep these four things in mind:

1. Your problem is not as unique as you think.
2. You have more data than you think.
3. You need less data than you think.
4. There is a useful measurement that is much simpler than you think.

THE ADVICE	1. Quantify	2. Simplify	3. Inform
	Cyber risk can and should be measured through quantitative and probabilistic methods. Proven mathematical and statistical methods work even with limited data.	Cyber risk is business risk and should be modeled as such. Models allow practitioners to collaborate around likelihood and consequences using common vocabulary.	Focusing on the organization's threats as they pertain to corporate objectives and crown jewels gets the whole organization on the same page about security priorities.

Transforming to Cyber Risk Quantification

Take, for example, the current state we outlined previously for companies using traditional risk assessment methodologies – in a matter of months, these companies can transform to employing cyber risk quantification.



The transformation lifecycle begins with training key stakeholders and defining a framework for discussing cyber risk within the organization and culminates with updated reporting based on the deployed probabilistic models.

In addition to training and awareness, another recommended approach to establishing cyber risk quantification as a better alternative is to initially use the methodology on a single decision that needs to be made – something that is relevant and involves cybersecurity risk. This gives an organization the opportunity to pilot cyber risk quantification in a contained and tangible way, but also results in a valuable output. Once the organization completes the pilot analysis, stakeholders can begin to socialize results and discover more use cases for risk-quantification capabilities. Many organizations have a lot of momentum in their cyber risk processes; transforming to cyber risk quantification is only successful when tangible benefits are brought to light early and often.

PILOT IN PRACTICE

Protiviti assisted a mid-sized life insurance company in piloting cyber risk quantification for a single-scope risk assessment to fulfill requirements of the New York Department of Financial Services (NYDFS) Part 500 cybersecurity regulation. The single scope of the assessment, and focus only on threats to non-public information, created a contained environment for piloting cyber risk quantification. Protiviti leveraged the FAIR model to frame and describe the assessed threat scenarios. Results of the assessment followed a common vocabulary, allowed for comparisons to be made across different threats, and ultimately fulfilled obligations of the regulation by providing insight to the organization on the impact of their cyber risk landscape. Internal stakeholders could articulate the methodology and defend the assessment to the board using the common language and explain the risk assessment process and results clearly to the regulator. The broad acceptance and understanding of the risk assessment results paved the way for the organization to deploy cyber risk quantification across a multitude of risk assessments and decision-making activities, with transformation continuing throughout the organization.

Why should an organization take the leap to cyber risk quantification?

Risk management is fundamentally about making decisions – and making those decisions becomes much easier when cyber risk is measured through quantitative methods. Cyber risk quantification is not a silver bullet preventing cyber attacks, but it is a useful tool.

Key Benefits of Cyber Risk Quantification
• Complete cyber risk assessments at a lower cost, with better results
• Prioritize security stack in monetary terms
• Determine the appropriate amount of cyber insurance
• Understand how much a breach would cost
• Clarify the return on investment for changes to the cybersecurity environment
• Increase the engagement of organization executives on cyber risk discussions
• Make better decisions and fulfill regulatory requirements

How Protiviti Can Help

Protiviti helps companies measure, quantify and report on risk by:

- Clearly defining a risk vocabulary and establishing a risk taxonomy to allow practitioners and the business to take a threats-based approach to cybersecurity risk and provide consistent risk register statements.
- Assessing cyber threats facing your organization using open quantitative risk measurement methodologies such as Applied Information Economics (AIE) and FAIR.
- Designing and implementing the programs and processes required to shift from a controls orientation of cybersecurity to a business risk orientation and optimizing compliance frameworks based on risks.
- Building cybersecurity datamarts to collect, process and store relevant metrics for analysis and reporting, including customized interactive reports and dashboards to replace legacy PowerPoint decks and spreadsheets.
- Conducting training and organizational change management to help your organization embrace a culture of data-driven informed decision-making.

Contacts

Scott Laliberte
+1.267.256.8825
scott.laliberte@protiviti.com

Andrew Retrum
+1.312.476.6353
andrew.retrum@protiviti.com

Vince Dasta
+1.312.476.6383
vince.dasta@protiviti.com