PeriCertum®

Risk Identification and Quantification

Solutions Overview

Risk Identification and Quantification

Prioritization And Budget

Predict and Prevent

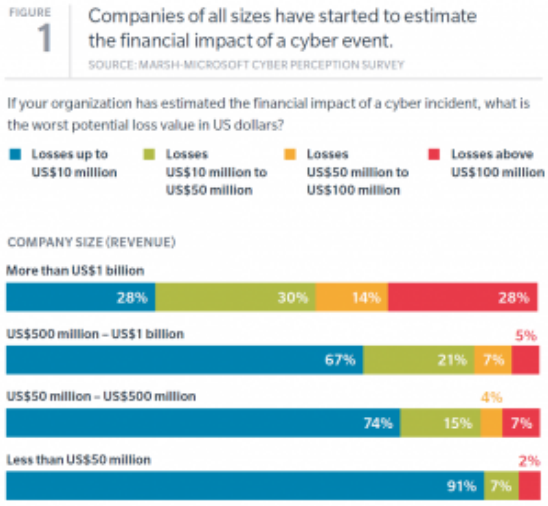
Risk Mitigation Solutions

Deep Assessment

Third Party Risk Scoring

Secure Cyber Operations

What is your cybersecurity risk?



Click to enlarge

In the last four decades, the world has experienced an enormous shift in where value lies. Consider that in 1975, just 17% of the market value of S&P 500 companies was tied to intangible assets, including data, intellectual property, and other technologies. The bulk of their value was in physical assets. Today, the numbers have reversed: Just 16% of value is in physical assets; the rest comes from intangibles.

This broad reliance on data and information extends to all companies — from automakers and aerospace giants to financial institutions and retail chains. As a result, organizations of all sizes and across all industries are vulnerable to cyber-attacks. And the threats are increasing not only in frequency, but are becoming more severe, diverse and complex, with significant consequences.

Despite these massive changes, most efforts in risk management and governance are still directed disproportionately toward legacy assets. Current efforts must also look at digital assets.

** The content above and the related image are referenced from the report, "By the Numbers: Global Cyber Risk Perception Survey," summarizing the results of the Marsh-Microsoft Cyber Perception Survey.*

How do you currently analyze cybersecurity risk?

Until recently, many organizations were limited to subjective evaluation of cybersecurity risk. These technique-based methods are unable to stand up to auditor and regulatory approval, due to their dependency on expert opinion and professional judgment.

We often run into home-built, handcrafted tools and spreadsheets. These tools are often difficult to maintain and rarely based on sound quantitative methods. Does your solution provide…

- **Financially literate results** – Valuation of the entire cybersecurity landscape of the enterprise to allow real-world profiling of the options and choices across the critical dimensions of the organization's actual cybersecurity conditions
- **Comprehensive traceability** – Detailed tracking of relationships between Threats, Risks, Vulnerabilities, and Capabilities provide for a thorough evaluation of the effects of the core variables of the cybersecurity program on one another
- **Cybersecurity – specific mathematical algorithm** –An objective valuation of risk effects, no longer dependent on factors of professional judgment or expert opinion of individuals by using probability density functions based on real-world cybersecurity attack data to derive insurance-grade risk profiles across 85 threat and vulnerability dimensions
- **Insurance-grade actuarial processes** –uses accepted actuarial principles to profile top risk categories against risk outcomes and financial impacts for your organization based on consultation with top cyber insurers, major-university economists and professional actuaries
- **Backtested threat profiling** – Using a catalog of over 104,000 detailed vulnerabilities, threat inputs are identified from your actual vulnerabilities, played back and tested against the comprehensive multi-year data of known threat actor patterns to derive mathematically correct probabilities as input to the valuation algorithm
- **Machine-learning based quantitative threat analysis** – Using a patented mathematical engine developed under DoD grants specifically for analyzing cybersecurity threats, our solution brings a reality-based understanding of issues of attacker budget, Darkweb market dynamics, and attack probability to your actual cybersecurity conditions

- **Strict adherence to regulator-derived descriptions and definitions throughout**– By operating within prevailing regulatory frameworks, we provide regulator-correct results to enhance compliance sign-off, while preserving regulator-derived descriptions and definitions throughout

Our solution, Thrivaca™ (an Arx Nimbus product) provides all of this.

Understanding your financially quantified Cyber Risk

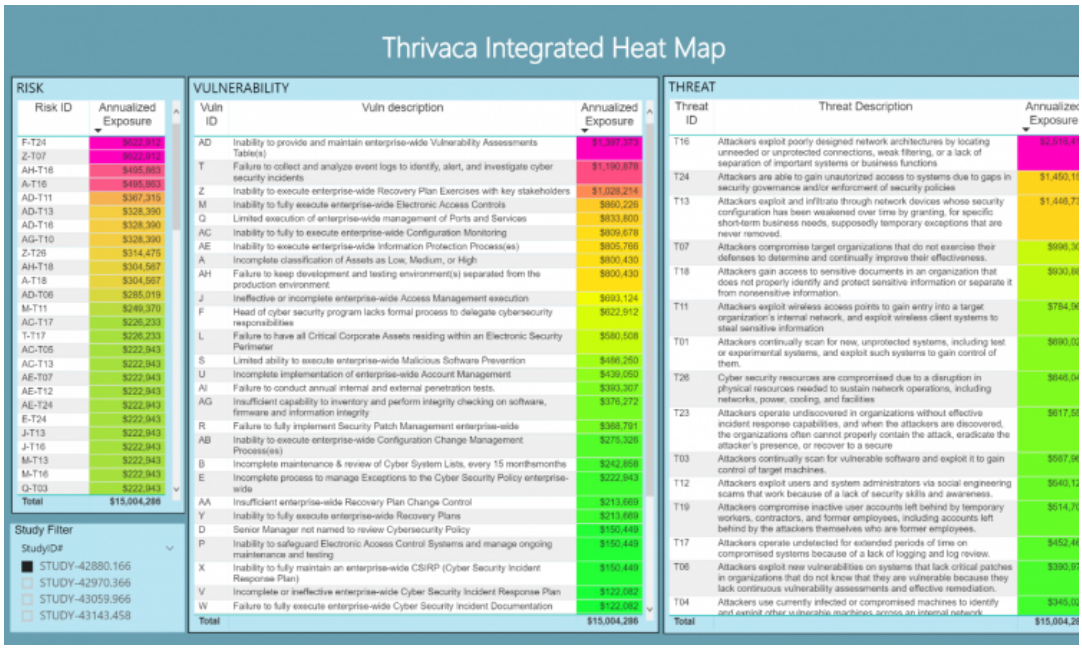
Click to enlarge

Threats. Risks. Vulnerabilities. Capabilities. These are the primary variables in understanding the most rapidly emerging issue for every organization today: **Cybersecurity**.

The Securities and Exchange Commission ("SEC") recently provided interpretive guidance (effective February 26, 2018) which substantially expands on the SEC's 2011 guidance on cybersecurity-related disclosures. The SEC states that companies must assess the materiality of any cybersecurity incidents that may occur, as well as any existing cyber-related risks when it prepares and files disclosures under securities laws.

Arx Nimbus' Thrivaca™ analytical platform provides the first detailed and quantitatively accurate map of the cybersecurity initiatives of the enterprise, the relevant regulatory compliance requirements, and prioritized high-impact risks, all against attainable capabilities, using the most recent quantitative

innovation and science from current research. The Thrivaca™ analytical platform provides a business-based, monetary valuation for the critical decisions in the definition of your cyber prevention roadmap. Consideration of timing, build vs. buy, and results are all delineated in dollars and cents, allowing for informed and transparent decision-making.



Click to enlarge

Questions

- How do I gain actual knowledge of my organization's cybersecurity risks?
- What are my top cybersecurity risks, and what is their relative financial impact?
- What is the value of acquiring specific cybersecurity capabilities?
- How can I profile probabilities of various risk scenarios?
- How would my current risk analysis processes, and the decisions they are being used to drive, stand up in a courtroom litigation scenario?
- How do risk-related measures like cyber insurance impact the organization?

Contact us today to see how we can help you identify and financially quantify your Cyber Risk.

Contact Us

CyberRisk

855-PCERTUM (855-723-7886)

PeriCertum on Linkedin

Evaluate Your Risk

SOLVE YOUR CYBER RISK

- Solutions Overview
- Risk Identification and Quantification
- Prioritization And Budget
- Predict and Prevent
- Risk Mitigation Solutions
- Deep Assessment
- Third Party Risk Scoring
- Secure Cyber Operations

OFFICES

Michigan Office
4301 Orchard Lake Road, Suite 180-177
West Bloomfield, MI 48323

Tennessee Office
II Brentwood Commons Suite 150
750 Old Hickory Boulevard
Nashville, TN 37027