FROST & SULLIVAN

BEST PRACTICES

AWARDS

FROST & SULLIVAN

2020 BEST PRACTICES AWARD

Cyberwrite

2020 GLOBAL CYBER RISK MODELING
TECHNOLOGY INNOVATION LEADERSHIP AWARD

Contents

Background and Company Performance

Industry Challenges

Companies need to protect their digital ecosystem against multiple threats, and while attackers need to find only one security flaw, companies must conduct an effective, consistent data-driven security program to prevent a cyber disaster. Small and large companies suffer from cybersecurity damages, and the financial impact of such incidents may cause business operations to cease. Cyber damages have grown exponentially in the last decade as a broadening digital and Internet-connected ecosystem raises a business's cyber risk. Even in cases where protection measures and mechanisms are deployed, the ever-evolving cyber risk posed to information technology (IT) systems, employees, and third-party vendors threaten an organization's business operations. Ultimately, a business is the custodian of its data and the data of its customers. Losing such data may result in financial fines, loss of business, and, in some cases, business closure. With the trend of remote work practices on the rise, organizations' IT teams struggle to identify risks, make sense of the data they see, and convert it into meaningful business decisions related to cyber insurance, vendor risk management, and IT posture.

Less than 50% of companies globally are equipped to mitigate cyber-attacks as security spending is insufficient to deal with the endless attacks and digital hazards.[1] Organizations globally are ill-prepared, especially considering the frequency of ransomware attacks alone will reach 11 seconds by 2021, and the expected total global cost of cyberattacks will reach $90 trillion by 2030.[2,3] More than 73% of companies are testing use cases for artificial intelligence (AI) in cybersecurity to combat the increasing number of cyber-attacks.[4] Still, most are not fully equipped to deal with AI-led cyberattacks utilized by cybercriminals.

One AI-powered cybersecurity application is cyber risk quantification to determine a company's technical and financial exposure to cyber breaches. Many organizations believe cyber risk assessments are single occurrences; however, as cyber postures may change daily, such assessments need to be periodic or, at minimum, event-triggered—e.g., a software update or other IT changes. A major challenge with legacy cyber risk assessments is that they only consider organizational preparedness and not inherent risks to the industry and geography in which a business operates. Semi-manual analysis conducted by consulting companies is ineffective as there is too much data to be analyzed in too little time. In such use-cases, AI and machine learning (ML) implementation lead to significant positive results.

Another contributing factor to automated cyber risk quantification is that many organizations find themselves lagging with too much to do, too few resources, and too little time due to existing methodologies. There is a massive shortage of experts across the security market, and the skyrocketing costs required to fill this gap exacerbates

---

[1] The Future of Privacy and Cybersecurity, Forecast to 2030 (Frost & Sullivan, June 2020)
[2] Cisco/Cybersecurity Ventures 2019 Cybersecurity Almanac
[3] Study published by Atlantic Council and the Zurich Insurance Group
[4] Capgemini Research Institute: Reinventing Cybersecurity with Artificial Intelligence

cybersecurity issues. Frost & Sullivan's research suggests that the demand for cybersecurity professionals will exceed supply by more than five times by 2025 as technologies move from a reactionary approach to a proactive approach.[5]

To protect business operations, managers must understand the financial impact a cyber-attack will have on their own business and the business of their 3rd party vendors. Implementing the right type of solutions, purchasing the right amount of cyber risk insurance policy coverage, and getting actionable and easy-to-use insights in a real-time and continuous manner is key to protecting businesses from intentional and accidental cyber attacks.

Cyber risk insurance policies are often one-size-fits-all, leaving small to medium-sized businesses (SMB) and companies in high/low-risk industries to customize their insurance coverage by guessing their financial cyber risk. However, many companies do not realize the full extent and magnitude of the potential monetary damages caused by cyber risks such as business interruption, ransom events, and regulatory fines. Thus, decision-makers are unable to choose adequate protection measures and insurance coverage due to limited data and lack of resources, often resulting in a hefty price tag and spending over-allocated budgets.

Cyber breach insurance premiums will increase tenfold to $20 billion annually by 2025 due to exposure to new and complex types of cyber threats.[6,7] Thus, businesses will need technology, more than ever, to drive decision-making related to the protection of IT and business systems, and utilize advanced cyber risk modeling technologies to optimize their cyber protection and insurance coverage.

Cyber risk modeling companies enable organizations to discover their cyber risk and translate it into financial terms—i.e., how much the organization's security vulnerabilities could cost the company (e.g., fines and other breach-related costs)—for multiple purposes. However, many cyber risk modeling companies cannot analyze and quantify the financial impact of cyber risks on companies effectively and do not possess capabilities that enable real-time and data-driven high-accuracy risk modeling. The use of AI and ML-powered analytics is critical to provide businesses with an accurate predictive cyber risk score or financial damage estimations. Frost & Sullivan's research finds that companies of all sizes across industries can benefit from deploying a cyber risk modeling solution that provides accurate cyber and financial risk figures through advanced AI and ML capabilities and predictive analytics.[8]

Technology Leverage and Business Impact of Cyberwrite

Founded in 2017, Cyberwrite is a US-based cyber risk modeling company with a research and development excellence center in Israel. The company leverages extensive experience and expertise in cyber risk modeling and actuarial science to develop industry-leading

---

[5] The Future of Privacy and Cybersecurity, Forecast to 2030 (Frost & Sullivan, June 2020)
[6] Allianz Global Corporate & Specialty SE
[7] The Future of Privacy and Cybersecurity, Forecast to 2030 (Frost & Sullivan, March 2020)
[8] Ibid

 "We Accelerate Growth"

cyber risk technologies to clients around the globe. The company embeds AI and ML algorithms and predictive analytics in its solutions to quantify cyber risk, empowering clients to implement effective measures in a data-driven, prioritized manner based on business data to protect them from potential financial damages. Customers may also use such information to acquire cyber insurance coverage that best suits their organization risk, allowing them to achieve a high return on investment (ROI). Cyberwrite serves customers in the United States, Europe, the Far East, and Australia through its global representatives and direct-sales force.

Cyberwrite's Revolutionary Cyber Risk Quantification & Mitigation Platform
Cyberwrite's real-time, on-demand Cyber Risk Quantification & Mitigation Platform quantifies cyber risk in financial terms that anyone can understand, from a business owner to an organization's IT professional to the chief executive officer and members of the board. The company's ML-based algorithms and actuarial science-powered solution help users understand the potential financial costs a business entity may face due to cyber threats and financial exposures to a third-party cyber breach while enabling decision-makers to be proactive and make data-driven decisions regarding their organization's cybersecurity. Cyberwrite's technology specializes in cyber profiling small- and medium-sized organizations and is also suitable for larger corporations across various use cases.

The following are key differentiating features of Cyberwrite in the cyber risk modeling market:

- **A risk model that considers the inherent risk of a company:** including geography, sector, and operational risk. Many cyber risk modeling companies offer a report that provides a score based on their review of an entity's IT posture. However, this process does not consider other risk factors outside of the organization's control. For example, a company may score higher on maintaining an effective IT security posture, but has valuable financial information belonging to US residents and operates in a sensitive region. Thus, even if they are doing well on security, their risk is still high and would not reflect on most competitors' reports. Cyberwrite's models indicate the actual risk of a company considering both the security posture and external risk factors. A comparison in the real world would be a country's risk. A country may have highly effective embedded security, but may still be at high risk due to the region it is located in, the surrounding counties, and additional factors. High security does not guarantee low risk.

- **Financial analysis of exposure to third parties:** Cyberwrite's predictive models enable the calculation of the potential financial damages caused by an engagement with a vendor, insuring a business for cyber risks, or an internal business unit's exposure. Such calculation is the missing piece in many risk modeling solutions commercially available today. This capability enables business decisions based on IT posture and actual business and financial factors.

- **On-demand profiling:** the Cyberwrite platform can profile on-demand any company across different geographies. Even if the company is not currently in the pool of

companies Cyberwrite has already profiled, it can be added within minutes by any non-technical user. Moreover, Cyberwrite is one of the only solutions that can profile micro-companies and provide a financial loss estimation to such companies.

The above differentiating factors make Cyberwrite a unique solution in a market that typically focuses on IT monitoring instead of risk monitoring.

In the cyber insurance market, many companies are left in the dark concerning their appropriate cyber insurance coverage limits. This is because both insurance brokers and their clients lack the technical skills to assess cyber risks for clients. The clients, in turn, struggle to convert raw cybersecurity data into an effective action plan and quantify the risk in financial terms. This may result in substantial security breaches, regulatory fines, ransom demands, and business interruption, which may lead to significant financial losses, loss of customer trust, and even bankruptcy. Many organizations fail to seek the right type of cyber risk coverage they need.

Recognizing this lack of data and cyber technical skills most businesses face, Cyberwrite created a technology that collects cyber risk-related data in real time and converts it into easy to understand reports that businesses and insurance companies can use to quantify potential damages and mitigate cyber risks. Cyberwrite started its journey by providing data and analytics to insurance companies, which are used for customer engagement, catastrophe modeling, and the underwriting of cyber risk policies for businesses worldwide.

Cyberwrite's unique process consists of three comprehensive steps: data collection, risk profile benchmarking, and financial impact estimation. Cyberwrite's technology can include new and updated risk scenarios per customer needs—a platform tailored to the risks they face. Cyberwrite's solution provides an around-the-clock, real-time dashboard to keep cybersecurity staff and C-level executives abreast of the organization's risk posture. The solution automatically collects data from all around the Internet, including the dark web and proprietary cyber risk and digital risk-related data related to each entity, which is used as classifiers in its exclusive ML models. Data regarding historical breaches is also collected to construct a comprehensive cyber risk benchmarking report for the entity based on historical events and is used as part of the ML algorithms.

Cyberwrite's technology also considers inherent risk factors, such as geography, industry, operational factors, and prior cybersecurity incidents such as stolen credentials, malware infections, cybersecurity readiness, attack surface, and digital exposure, to generate a unique cyber-risk profile for each entity on its platform. All the data is converted in real time into a one-page, easy to understand risk report that includes a comprehensive intelligence and data gathering report and actionable recommendations—all within minutes and ready to be used by non-technical users as well as IT departments. These reports can be generated at time intervals suited to the needs of each customer.

Cyberwrite's predictive analytics algorithm serves as a significant differentiating factor; it calculates the likelihood of a cyberattack specific to the client and the type and size of financial damages resulting from such an attack. This enables customers to select

appropriate protection measures and insurance coverage that reflects their business needs, and proactively reduces their cyber risk. Furthermore, the company's easy-to-read dashboard comprises a risk score ranging from 1 to 100, representing low to high risk to enable anyone from the IT team to C-level executives understand their organization's risk levels.

Cyberwrite also provides insurance companies with a dedicated underwriting tool tailored to their risk appetite, which includes an actuarial score and probable financial impact for each customer as well as a benchmarking score that compares the business to similar companies from the same industry and geography. This real-time, end-to-end solution includes data collection, historical incident mapping, generation of actional mitigation reports, financial risk assessment, and industry benchmarking requires zero integration from Cyberwrite's customers.

Use Case Demonstrating Cyberwrite's Value

As cybercriminals' tactics continually evolve to overcome advanced cybersecurity technologies, regulatory agencies introduce additional industry standards—e.g., the General Data Protection Regulation—that organizations must implement to protect their business against cyber events and hefty penalties. However, many companies, SMBs in particular, are ill-equipped—on a financial and technical level—to manage cyber readiness to a sufficient degree. Cyberwrite's platform arms such companies with the knowledge required to understand risk exposures, calculate potential damages, get real-time recommendations tailored to their biasness and obtain an optimized insurance policy that will enable them to cover damages related to a cyber-attack, rather than drown in the chaos.

Moreover, the company's solution assists insurance companies with retaining customers and providing policies that align with their clients' requirements. For example, large global insurance firms use Cyberwrite's solution to underwrite cyber risk insurance policies for SMBs, enabling their agents and brokers to explain financial damages to customers for engagement purposes. The company's platform allows businesses to mitigate cyber vulnerabilities and risks proactively and acquire coverage to protect the business from financial consequences resulting from a cyber breach. The insurance company engages clients to provide a comprehensive view of their security posture via Cyberwrite's comprehensive cyber risk reports. Cyberwrite also provides the insurance firm with a dedicated underwriting report tailored to their coverage and risk appetite. It also helps offer an insurance policy fitted to the customer's needs while saving operational expenditures and allowing them to achieve a high ROI. Cyberwrite's solutions can help the insurance firm gain their clients' trust and loyalty by providing insurance policies that optimize the customer's protection needs, resulting in high customer satisfaction.

Corporations also use Cyberwrite's solution for vendor risk management, ongoing monitoring of cyber risks, and online monitoring of risks associated with third parties. The advantage of assessing and scoring risks, not only IT posture, enables corporates that require a third-party vendor platform to understand their financial exposure to vendors due to cyber risks, which is a differentiating factor in this market. An organization may

monitor the overall financial cyber exposure it has due to vendor engagement and monitors it over time. Cyberwrite's combination of actionable risk data, historical data, and predictive analytics make it a technology innovation leader in cyber risk modeling.

Exceptional Customer Support and Market Understanding Driving Cyberwrite's Growth

Cyberwrite works closely with corporates, insurance companies, insurance brokers, business owners, risk managers, underwriters, actuaries, and consulting firms to help businesses quantify their organization's financial cyber risk and mitigate it. The company offers unparalleled customer service by working closely with clients to ensure they understand their cyber risk score and the financial impact. Moreover, Cyberwrite also provides resources on the cyber risk market and its clients' industries regarding cyber risk modeling, cyber insurance, and financial cyber risks. One of its customers stated:

> *"In a market where data quality is substandard, Cyberwrite is incredibly useful in augmenting our cyber data. The team is very keen to learn and share their cybersecurity knowledge and provide a tailored solution that meets customers' requirements. Cyberwrite is a reliable and progressive company that adds value through data augmentation, particulary for an SME book of business."*

As a company in a nascent market, Cyberwrite understands the challenges it faces in the cyber risk modeling and profiling industry regarding gaining customers' trust while providing accurate and actionable data on an ever-evolving environment. The market faces three main challenges; Cyberwrite's approach to overcoming these challenges positions it as an industry leader in this market:

> ***How to automatically collect accurate and significant underlying data and generate a simple to understand risk report in minutes***: Cyberwrite collects publicly available and customer proprietary cyber risk data to create risk scores and benchmarking via AI and ML algorithms. The company only uses algorithms that it can make sense of while many competitors deploy algorithms without full visibility on how they calculate risk, and thus, they cannot explain to their customers how the solution calculates cyber and financial risk scores. To this end, Cyberwrite does not focus on a rapid adoption of new AI algorithms, ensuring its solution remains precise in its data collection, analysis, and cyber risk scores.

> ***How to conduct meaningful analytics in a cost-efficient manner by using customized cyber risk modeling and profiling using ML and AI:*** Cyberwrite's advanced analytics finds a correlation between data and historical cyber damages, which is used by insurance companies and organizations globally. Top-tier experts have reviewed its models, and its customers' renewal of engagement year after year is a testament to its success in solving this challenge. Furthermore, Cyberwrite does not sell insurance or cybersecurity services, which helps maintain its objectivity as an independent risk modeler. The company acquires customers by proving unmatched value through its solutions to businesses and insurance companies.

> ***How to mitigate the risk posed to the business and enable better protection of digital assets and business operations:*** Cyberwrite's platform provides future insights through its predictive analytics of probability and potential financial losses. These insights are used to acquire accurate data and provide actionable recommendations for clients to fix security issues and potentially attain a cyber insurance policy that fits their business requirements. Moreover, Cyberwrite enables clients to pinpoint ecosystem vulnerabilities, allowing security teams to remediate system gaps and make sure business executives understand the potential impact of a cyber incident and budget remediation actions.

Serving as a testament to Cyberwrite's game-changing technology and outstanding customer support, it achieved triple growth in 2019 and expects to accomplish this impressive growth again in 2020. Aligning with the company's global expansion, Cyberwrite's platform is available in multiple languages, including English, Italian, Japanese, Portuguese, French, and more. The company is actively working on adding new languages.

Conclusion

Most companies lack the knowledge and budget to conduct ongoing self-assessment of cyber risks. Cyberwrite's technology enables any business to make sense of an immense amount of data, reduce costs in the process, and benchmark their risks to similar companies. Modeling financial damages caused by cyber risks empowers management personnel to make investment decisions in cyber protection and cyber insurance. Cyberwrite's cyber risk modeling platform enables businesses to quantify their risks in terms of the financial costs associated with a cyber-attack and adjust the cyber insurance limits required to protect their organization. In particular, small to medium-sized businesses (SMBs) can leverage Cyberwrite's reports to acquire cost-effective information and knowledge previously available only to large corporations with larger cyber risk mitigation budgets, enabling SMB's to buy an insurance coverage tailored to their specific needs.

Insurance firms also use Cyberwrite's platform on a day-to-day basis to underwrite cyber insurance policies across industries, explain risk exposures to clients and support them in risk remediation, resulting in customer engagement, business, and loyalty. Cyberwrite equips its revolutionary solution with tailored artificial intelligence and machine learning algorithms and predictive analytics, which results in unprecedented accuracy for clients.

With its unmatched technology innovation, customer-centric approach, trustworthiness among its customers, and strong overall performance, Cyberwrite earns Frost & Sullivan's 2020 Global Technology Innovation Leadership Award in the cyber risk modeling industry.

Significance of Technology Innovation Leadership

Technology-rich companies with strong commercialization strategies benefit from the increased demand for high-quality, technologically-innovative products. Those products help shape the brand, leading to a strong, differentiated market position.

Understanding Technology Innovation Leadership

Technology Innovation Leadership recognizes companies that lead the development and successful introduction of high-tech solutions to customers' most pressing needs, altering the industry or business landscape in the process. These companies shape the future of technology and its uses. Ultimately, success is measured by the degree to which a technology is leveraged and the impact that technology has on growing the business.

Key Benchmarking Criteria

For the Technology Innovation Leadership Award, Frost & Sullivan analysts independently evaluated two key factors—Technology Leverage and Business Impact—according to the criteria identified below.

Technology Leverage

Criterion 1: Commitment to Innovation
Requirement: Conscious, ongoing development of an organization's culture that supports the pursuit of groundbreaking ideas through the leverage of technology.

Criterion 2: Commitment to Creativity
Requirement: Employees rewarded for pushing the limits of form and function by integrating the latest technologies to enhance products.

Criterion 3: Technology Incubation
Requirement: A structured process with adequate investment to incubate new technologies developed internally or through strategic partnerships.

Criterion 4: Commercialization Success
Requirement: A proven track record of commercializing new technologies by enabling new products and/or through licensing strategies.

Criterion 5: Application Diversity
Requirement: The development of technologies that serve multiple products, multiple applications, and multiple user environments.

Business Impact

Criterion 1: Financial Performance
Requirement: Overall financial performance is strong in terms of revenue, revenue growth, operating margin, and other key financial metrics.

Criterion 2: Customer Acquisition
Requirement: Overall technology strength enables acquisition of new customers, even as it enhances retention of current customers.

Criterion 3: Operational Efficiency
Requirement: Staff is able to perform assigned tasks productively, quickly, and to a high quality standard.

Criterion 4: Growth Potential
Requirements: Technology focus strengthens brand, reinforces customer loyalty, and enhances growth potential.

Criterion 5: Human Capital
Requirement: Company culture is characterized by a strong commitment to customer impact through technology leverage, which enhances employee morale and retention.

Best Practices Recognition: 10 Steps to Researching, Identifying, and Recognizing Best Practices

Frost & Sullivan Awards follow a 10-step process to evaluate Award candidates and assess their fit with select best practice criteria. The reputation and integrity of the Awards are based on close adherence to this process.

STEP		OBJECTIVE	KEY ACTIVITIES	OUTPUT
1	**Monitor, target, and screen**	Identify Award recipient candidates from around the globe	• Conduct in-depth industry research • Identify emerging sectors • Scan multiple geographies	Pipeline of candidates who potentially meet all best-practice criteria
2	**Perform 360-degree research**	Perform comprehensive, 360-degree research on all candidates in the pipeline	• Interview thought leaders and industry practitioners • Assess candidates' fit with best-practice criteria • Rank all candidates	Matrix positioning of all candidates' performance relative to one another
3	**Invite thought leadership in best practices**	Perform in-depth examination of all candidates	• Confirm best-practice criteria • Examine eligibility of all candidates • Identify any information gaps	Detailed profiles of all ranked candidates
4	**Initiate research director review**	Conduct an unbiased evaluation of all candidate profiles	• Brainstorm ranking options • Invite multiple perspectives on candidates' performance • Update candidate profiles	Final prioritization of all eligible candidates and companion best-practice positioning paper
5	**Assemble panel of industry experts**	Present findings to an expert panel of industry thought leaders	• Share findings • Strengthen cases for candidate eligibility • Prioritize candidates	Refined list of prioritized Award candidates
6	**Conduct global industry review**	Build consensus on Award candidates' eligibility	• Hold global team meeting to review all candidates • Pressure-test fit with criteria • Confirm inclusion of all eligible candidates	Final list of eligible Award candidates, representing success stories worldwide
7	**Perform quality check**	Develop official Award consideration materials	• Perform final performance benchmarking activities • Write nominations • Perform quality review	High-quality, accurate, and creative presentation of nominees' successes
8	**Reconnect with panel of industry experts**	Finalize the selection of the best-practice Award recipient	• Review analysis with panel • Build consensus • Select recipient	Decision on which company performs best against all best-practice criteria
9	**Communicate recognition**	Inform Award recipient of Award recognition	• Announce Award to the CEO • Inspire the organization for continued success • Celebrate the recipient's performance	Announcement of Award and plan for how recipient can use the Award to enhance the brand
10	**Take strategic action**	Upon licensing, company is able to share Award news with stakeholders and customers	• Coordinate media outreach • Design a marketing plan • Assess Award's role in future strategic planning	Widespread awareness of recipient's Award status among investors, media personnel, and employees

The Intersection between 360-Degree Research and Best Practices Awards

Research Methodology

Frost & Sullivan's 360-degree research methodology represents the analytical rigor of our research process. It offers a 360-degree-view of industry challenges, trends, and issues by integrating all 7 of Frost & Sullivan's research methodologies. Too often companies make important growth decisions based on a narrow understanding of their environment, leading to errors of both omission and commission. Successful growth strategies are founded on a thorough understanding of market, technical, economic, financial, customer, best practices, and demographic analyses. The integration of these research disciplines into the 360-degree research methodology provides an evaluation platform for benchmarking industry players and for identifying those performing at best-in-class levels.

360-DEGREE RESEARCH: SEEING ORDER IN THE CHAOS

About Frost & Sullivan

Frost & Sullivan, the Growth Partnership Company, enables clients to accelerate growth and achieve best-in-class positions in growth, innovation and leadership. The company's Growth Partnership Service provides the CEO and the CEO's Growth Team with disciplined research and best practice models to drive the generation, evaluation and implementation of powerful growth strategies. Frost & Sullivan leverages more than 50 years of experience in partnering with Global 1000 companies, emerging businesses, and the investment community from 45 offices on six continents. To join our Growth Partnership, please visit http://www.frost.com.