

A background network diagram consisting of numerous dark grey nodes connected by thin lines, set against a gradient background transitioning from light purple on the left to light orange on the right. The nodes are arranged in a complex, interconnected pattern, resembling a web or a data network.

MeasuredRisk

Investment Brief
February 2019

The highly dynamic global business environment, combined with geopolitical shifts, rapidly emerging technologies, cyber threats, economic and financial market volatilities, tax reform and other emerging developments create tremendous opportunities for organizations as they pursue growth and the advancement of their core mission. As business leaders manage their ever-changing economic, political, and technological landscape they face an exponentially increasing range of uncertainty that creates a highly complex portfolio of potential risks that, if unmanaged, can cripple, if not destroy, and organization's business model and brand.

- 2018 The State of Risk Oversight¹

OVERVIEW

Organizations today face an array of risks more complex and severe by many orders of magnitude than ever before. With globalization, companies around the world must now understand and counteract a vast web of operational, economic, social, environmental, and geopolitical risks. Among these, cyber risks have emerged as arguably the most predominant and pernicious.

Although there are many technologies available to help companies identify and assess individual indicators of risks, very few can connect all the dots and provide a meaningful holistic picture of multiple asynchronous risks in order to effectively diminish or even neutralize their impact. In addition, though prioritizing business leaders' access to critical information and ability to make real-time decisions is paramount to rectifying one common cause of subpar enterprise risk mitigation, there are no other solutions specifically oriented toward the C-Suite. Identifying these sorts of deficiencies in the market and recognizing the compelling need for a platform that can connect and analyze every risk indicator and also enable business leaders to make risk-related decisions in the business context, led to the genesis of MeasuredRisk. Founded in 2015, MeasuredRisk is dedicated to redefining how companies see risk.

Headquartered in Arlington, VA, MeasuredRisk is the brainchild of Tom Albert, who is well-known as the 'go-to-guy' in risk management and cybersecurity through his extensive experience and impressive track record. Under Albert's leadership, the company nurtures a culture of multi-disciplinary diversity, bringing together world-class experts from across cybersecurity, IT operations, business continuity, geopolitics, international intelligence, human factors analysis, and big data analytics. This collaborative approach is key to helping different business functions within an organization mitigate impending risk, and more effectively absorb and nimbly respond to the impact of unavoidable risk.

MeasuredRisk was created to solve one of the world's most complex problems around asserting the implications of risk, in real time, for organizations that operate around the globe.



Insider Threat



Legal



Brand



Operational



MeasuredRisk tracks eight key risk indicators, continuously, for clients expertly chosen for their relevance in keeping a company's interests secure.



Infrastructure



Economic



Proficiency



Geopolitical

¹ An Overview of Enterprise Risk Management Practices – 9th Edition. March 2018.

INVESTMENT

We are raising up to \$5,000,000 through a "Pre-Sale" of security tokens at a price of \$1.00 per token ("Offered Tokens"). The Offering is being made pursuant to an exemption from registration under Rule 506(c) of Regulation D of Section 402(a)(2) of the Securities Act.

Use of proceeds for the Offered Tokens will be applied to further development of the Measured Risk platform, establishing a formal sales and marketing program and working capital.

Use of Proceeds		Max
Research and Development	\$	300,000
General & Administrative		3,650,000
Marketing and Sales		1,000,000
Offering Expenses		50,000
Total	\$	5,000,000

We believe the maximum Offered Tokens will be sufficient to sustain our operations for the foreseeable future.

Offered Tokens and Tokenomics

Key Offering Data	Max	Tokenomics	
Corporate Structure		Tokens	5,000,000
Shares Out	6,450,000	Royalty Rate	7%
Warrants/Options Out	5,100,000	<i>Token Conversion to Common</i>	
Convertible Debt	\$ -	Tokens per Share	5
Shares issued on Debt Conv.	-	Implied Underlying Shares on Full Convert	1,000,000
Shares Out Fully Diluted	11,550,000		
Securities Token Offering (STO)	\$ 5,000,000		
Offering Price / Token	\$ 1.00		
Offered Tokens	5,000,000		
Post Offering Shares Out (FD)	11,550,000		
Post Offering Tokens Out (FD)	5,000,000		

Each security token will provide token holder with a pro-rata share of gross 7% of the Company's revenues (the "Royalty" payment), and each five (5) security tokens held by token holder are convertible, at the sole discretion of the token holder, into one (1) share of MeasuredRisk common stock, par value **. ²

Hypothetical Royalty Distribution and ROI Analysis to Series A Token Holders

(based on pro forma revenue forecast)

	2019	2020	2021	2022	2023
Shares Out	11,550,000	11,550,000	11,550,000	11,550,000	12,550,000
Token APIC	\$ 5,000,000				
Converted Share Implied Val.	\$ 62,750,000				
Tokens Out	5,000,000	5,000,000	5,000,000	5,000,000	5,000,000
Enterprise Value	\$ -	\$ 52,300,000	\$ 266,200,000	\$ 670,200,000	\$1,411,700,000
Implied Share Price	\$ -	\$ 4.53	\$ 23.05	\$ 58.03	\$ 112.49
Token Royalties	\$ 296,800	\$ 1,264,200	\$ 3,266,200	\$ 6,867,000	\$ 12,857,600
Token Royalties Cumulative	\$ 296,800	\$ 1,561,000	\$ 4,827,200	\$ 11,694,200	\$ 24,551,800
Token ROI (Royalty Only)	-94.1%	-68.8%	-3.5%	133.9%	391.0%
Converted Share ROI	-100.0%	-16.7%	324.2%	968.0%	2149.7%

² Exception case. In the case that the Company goes public, is acquired by or merged with another company, the tokens held will automatically be converted into underlying shares of the Company's common stock at a 5:1 ratio.

Connecting the Dots

While most players in the market only focus on cyberthreats, MeasuredRisk differentiates itself with a technology architecture that allows the company to harvest both raw and transformed data from multiple disparate sources. After gathering structured and unstructured data from both original source and third-party technologies, and covering many categories of risk, the company's software-as-a-service (SaaS) platform distills information specifically relevant only to any given organization.

The more typical, myopic approach to collecting and viewing data fails to give a broader picture covering the entire spectrum of risk categories. By contrast, MeasuredRisk focuses on connecting the different data points by networking key risk indicators and mapping them to business-specific criteria. Designed for C-Level consumption, MeasuredRisk's comprehensive business risk management platform leverages statistical modeling and multi-disciplinary subject matter expertise to help business functions collaborate, enabling business leaders to make informed risk decisions. Albert points out that the conventional approach taken by the vast majority of solution providers is to provide an inside-out view of an organization's risks. MeasuredRisk's dynamic risk model, on the other hand, presents a multi-brand organization with an outside-in view of multiple risks, ranging from cyber, operational, economic, social, environmental, and geopolitical, whether local, regional, global, or a combination of all.

Artificial Intelligence to Mitigate Real Risk

One of the biggest differentiators for MeasuredRisk is that while most solutions in the market are inherently dependent on integration into an organization's IT infrastructure to function, MeasuredRisk can provide a hawk's eye view into an organization's risks even before they formally sign contracts. Other alternatives typically depend on integrating with their client's IT infrastructure are susceptible to myriad problems and might actually increase risk vulnerabilities. These predictably include situations where the systems don't integrate as expected or information exchange fails, and organizations end up with a very complex, and often expensive, system which doesn't properly depict their risks. CEO Tom Albert, says that "We have taken a different route where we first take in the bulk of data of organizations and make determinations about those organizations to engage with them with a very clear mind and a picture of what their risk is."

Transforming the way organizations view and approach risk

To achieve this, MeasuredRisk leverages the power of machine learning and other forms of artificial intelligence (AI) as tools to mitigate and forecast an organization's risks.

As of today, the company's repository holds data from over 30 million companies to which it applies the most leading-edge capability of graph database showing 286 million edges of data,

Platform

MeasuredRisk View.

- The autonomous system navigates each organizations assets, dependencies and alliances. Data that often appears benign can prove to be nefarious when coupled with greater context.
- Using neural networks, MeasuredRisk View identifies the shape of risk by inspecting the traversal points and the structure of connective fabric between risk data. The process is continuous and learns the archetypes that represent organizational risk.
- View distills and prioritizes the most critical information in a way that is consumable by executives and leaders alike.

MeasuredRisk Pulse.

- Pulse is a multi-dimensional cyber risk assertion program that goes beyond solutions in the market today.
- Real-life defense determination, from the outside in.
- Dynamic vs. Static risk assertion.
- Multi-dimensional attack vector determination.
- Advanced Human and Artificial Intelligence to help organizations make the right defense investments for capital efficiency.
- Trust through ongoing awareness of organizational strengths and weaknesses.

Revenue Model

- Subscription-based (monthly and annual)

which together can measurably help companies make more robust connections and interpretations for efficient risk realization.

By harnessing the ability of machine learning models to analyze large amounts of data, MeasuredRisk's advisors help companies drive business efficiency and allow them to immediately see where the greatest risks lie. The advisory services offered by MeasuredRisk covers four core business elements— operations, finance, people, and brand—to holistically assess the multi-faceted array of risks companies actually confront. "We are building real-time decision support for leaders around the world empowering them to make determinations when they need to at that very time," states Albert.

Another distinguishing feature of MeasuredRisk's innovative approach to assessing and forecasting risks leverages psychodynamic intelligence analytics—soft and shadow data regarding the human element. Generally misunderstood, underestimated, and subordinated in value by most technology and advisory services firms, MeasuredRisk weights the human factor component as one of the most critical and impactful variables in the organizational risk matrix.

Creating a niche

An early indicator of MeasuredRisk's tremendous growth potential is that its platform is already being broadly used by companies outside its core offerings in traditional security. A large hospital system, for instance, leveraged MeasuredRisk's technology to enhance a derivative of one of its pre-existing medical monitoring systems, deploying it in its operating theatres to better assess the risks patients face while undergoing cardiac procedures. Another client is working with MeasuredRisk to address and mitigate the inherent risks of third parties they are doing business with. Yet another huge market opportunity that MeasuredRisk is focusing on is to white label their offerings. "This presents a humongous scope for our technology to penetrate markets around the globe," expresses Albert.

Envisioning the future, Albert expects MeasuredRisk to have multiple business units focus on verticals dealing with different problem spaces but all using deep learning as the foundational principle that will help organizations clearly determine and more accurately predict risk.

Albert also plans to leverage his expertise and the company's capabilities in deception technology—an emerging category of cybersecurity defense for risk mitigation. It is gaining popularity for its ability to detect, analyze, and defend against zero-day and advanced attacks, often in real time. By taking the less trodden path, MeasuredRisk is not only creating a niche for itself but leading a transformation of how organizations view and approach risks.

ARTIFICIAL INTELLIGENCE, MACHINE LEARNING AND RISK MANAGEMENT MARKET

A recent GARP survey³ on the risk management community to discover how artificial intelligence (AI) is being handled.

- The degree to which risk managers plan to make use of AI
- Whether they have any oversight of the risk of non-adoption in their organizations
- Whether they have a role in innovation risk at all

It found that

- AI adoption and capability are markedly high among a very small proportion of companies. Adoption and capability drop off quickly.
- Organizations tend not to understand their own data assets well enough to make good decisions about AI, making it difficult to build a case for investment from the C-suite.
- AI could be seen as a trigger for accelerating business process redesign, but it tends to feel like a threat, creating a fear of low performance that deters managers from taking new initiatives in the area.
- 33% of risk managers that responded to the survey believe AI is just one more innovation while 67% see it as a foundational change
- In the broader business community executives think AI will alter the way business is done

³ "Are Risk Managers Ready for Artificial Intelligence?". February 27, 2017. Global Association of Risk Professionals.

- Are you currently using AI in the risk management function of your organization?
 - o 76% No
 - o 15% Yes
 - o 9% Not sure
- 13% of respondents believe AI will become more relevant over the next 12 months; 41% believe it will happen in one to three years; and 46% say it is at least 3 years out
- Where does the risk management function get engaged in AI?
 - o 23% - in assessing the costs and risks of adoption
 - o 32% - in framing the economic argument for adoption or non-adoption
 - o 45% in analyzing the systemic risks of new technologies

Artificial intelligence and risk management perfectly align when there is a need in handling and evaluating unstructured data. It is estimated that risk managers will focus on analytics and stopping losses in a proactive manner based on AI findings, rather than spending time in managing the risks inherent in the operational processes.

AI solutions are able to fuel enterprises and businesses with trusted and timely data for building competence around their customer intelligence and successful implementation of their strategies.

Given the development of digital technologies and decreases in the cost of data storage, Artificial intelligence is becoming an integral part of business processes. Machine learning allows handling and analyzing unstructured data, thus saving time and money of for companies. AI in risk management can lower operational, regulatory and compliance costs and provide reliable credit scorings for credit decision makers. Risk assessment AI can provide a fast and accurate risk assessment, using every data - both financial and non-financial - it can find to factor in the character and capacity of a customer.

AI-powered risk management solutions can be also used for model risk management (back-testing and model validation) and stress testing, which is required by European and US prudential regulators.

Machine learning is the branch of AI most relevant for supporting risk-informed decision making as it focuses on discovering patterns in data and categorizing or predicting outcomes.

Like traditional business intelligence and predictive analytics tools, machine learning uses a variety of statistical methods. The range of methods are generally classified into: (1) *regression* analysis to determine independent and dependent variable relationships; (2) *classification* to identify and label dependent variables; and (3) *clustering* to discover the general characteristics of groups of observations without any predetermined dependent or independent variable.

Unlike traditional business intelligence and predictive analytics tools which use specifically chosen variables built on structured quantitative data, machine learning allows the flexibility to use unstructured data (not just quantitative) and the program determines variables and coefficients to use on its own.

The first two method categories (regression and classification) require supervised learning with outcomes scored and used as feedback to help train a program to refine its model. Clustering, in contrast, uses an unsupervised learning process that discovers patterns using neural networks with dynamically changing variables and weights as it churns its own modeled system to find key features of the given dataset.

Machine learning improves upon traditional business analytics tools given its ability to use a large variety and volume of information without any of the predetermined static relationships used in traditional models. The dynamics of machine learning allow it to constantly improve precision as it ingests more information. Information that may now include unstructured text (e.g. email and social media content), visual, and auditory inputs.

Given these qualities, machine learning can provide decision support by presenting likely outcomes while considering risk variables that are either initially known or unknown to decision makers in any business environment. Risk managers should welcome an innovative approach that can help address ambiguous variables, unstructured data, and unknowns.

The Challenges, Pros, and Cons of Implementing AI Tools for Risk Management

Awareness levels and cultural concerns typically pose the greatest organizational challenges for innovative technology adoption. They are the top challenges for the use of AI solutions in support of business decision making. Other concerns such as complexity and cost are dissipating for basic solutions. Open source algorithms are available for in-house development while many AI-based vendor software solutions offer free entry points for simple data sets to test its value for broader tasks.

Opting for in-house development will certainly require more time and expense as you acquire data engineering talent and run through machine training with multiple test cycles. But regardless of opting for a vendor service or an internally developed solution, implementation success will depend on your ability to assemble large data sets to train and refine models.

Some of the arguments for implementing AI to support risk-informed decision making include the following:

- The process of assembling data for machine learning will help expand the consideration of more risk factors in the context of specific business objectives.
- It will help embed risk identification and risk assessment in frontline decision-making processes.
- It will enable the use of a greater variety and volume of new data sets to help improve predictive capabilities.
- It will consider both structured and unstructured information.
- It will help reduce (but not eliminate) the model bias that is inherent in the choices of variables and coefficients used in static models.
- It will help extend risk considerations beyond just the core known risks and offer the potential for dynamically discovering new and emerging risks.
- Predictive capabilities will improve over time as input information grows.
- It will facilitate real-time risk identification and risk analysis.

Some of the factors that may weigh against implementing AI include:

- The cost and time to build and train unique models.
- The potential downside of using predicted outcomes from machine learning as *prescriptive decisions* rather than *considerations* for business decisions.
- The erosion of personal accountability for decisions associated with the prior point.
- The biases that may still exist from historical data selection for training and the choice of statistical algorithms used in the models.
- The challenge of communicating to decision makers that AI models will still provide probabilistic answers and should not be used as certainties.
- Current organizational standard practices, culture, and role responsibilities for risk management and auditing may have to adjust to accept new risk identification processes as well as documentation capabilities and limitations.
- The black box aspects of the clustering machine learning techniques, particularly those leveraging deep learning models, may not lend enough insights for the basis of decision making that must be documented to meet regulatory requirements.

The global AI market is expected to reach USD 35,870.0 million by 2025 from its direct revenue sources, growing at a CAGR of 57.2% from 2017 to 2025, whereas it is expected to garner around USD 58,975.4 million by 2025 from its enabled revenue arena⁴

⁴ "Artificial Intelligence Market Size to Reach \$35,870 Million by 2025." July 2017. Grandview Research.

RISK MANAGEMENT LANDSCAPE

The global risk analytics market was valued at USD \$9.15 billion in 2017 and is expected to reach \$19.31 billion by 2023⁵

The market is expected to move towards taking a unified approach to risk management and developing an integrated risk management solution to enable business units and functions to incorporate risk intelligence into the many actions they take across different business units. Deployment of these solutions over the cloud is expected to provide opportunities to SMEs to take better decisions. However, the cyber risks associated are the major factor restraining the deployment of these solutions over the cloud.

Cyber Risk Management. Business managers consider cyber risk to be the biggest threat to their business. With almost all businesses linked in some way to the Internet, the threat of cyberattack is almost universal.

- From 2011 to 2014 energy companies in Canada, Europe and the U.S. were attacked by the cyberespionage group Dragonfly;
- In 2017, WannaCry ransomware held hostage public and private organizations in telecommunications, healthcare and logistics, while NotPetya ransomware attacked major European companies in a wide variety of industries;
- In 2018, Meltdown and Spectre

A recent McKinsey report says only 16% of executives feel their companies are well prepared to deal with cyber risk.⁶ Expectations are that the threat of cyber risk will continue to increase as business continues to go digital, adapts new technologies including artificial intelligence, advanced analytics and the Internet of Things. Assets ranging from new product designs to distribution networks and customer data are increasingly at risk. Meanwhile, digital value chains are getting more complex.

Enterprise Risk Management. This sub-category includes companies that address broader risk types that impact more than one area of the enterprise, such as fraud risk. This includes Fenergo, a client life-cycle management platform that provides end-to-end regulatory onboarding and monitoring for fraud. This also includes Argos Risk, a web-based platform that helps companies manage credit risk and protect against business identity fraud. Other companies operating in this space include Cloud 9, Finomial and Qumram.

Vendor Risk Management. Companies in this category are providing software to automate, facilitate, and centralize the execution of a continuous vendor risk management program in accordance with regulatory guidance on third-party risk management. This guidance was established by global regulators to manage and mitigate the risk associated with outsourcing operations and to establish a vendor due diligence process. Companies in this category include Venminder, a suite of software and services to assess, monitor, and manage third-party vendor risks and CBANC Network, a platform for professionals to collaborate on vendor selections. Other companies operating in this space include Greenlight Guru, Invis Alert Solutions and Qualtrax.

Operations Risk Management. Companies in this sub-category provide software to manage the day-to-day operational risks of a financial services organization. This includes governance, risk mitigation, incident identification, issue tracking, monitoring for compliance obligations, data storage, and reporting. Companies in the ORM sub-category include Rsam, a provider of Governance, Risk and Compliance (GRC) software and NetGuardians, a risk management software that facilitates incident identification, tracking, and management. Other companies operating in this space include Coyrlitics and Ascent.

The principal competitive factors in our market include: product features, reliability, performance and effectiveness; product line breadth, diversity and applicability; product extensibility and ability to integrate with other technology

⁵ "Global Risk Analytics (Software, Services) Market to Grow from \$9.15 Billion in 2017 to \$19.31 Billion in 2023." May 16, 2018. Research and Markets.com.

⁶ A new posture for cybersecurity in a networked world. March 2018.

infrastructures; price and total cost of ownership; adherence to industry standards and certifications; strength of sales and marketing efforts; and brand awareness and reputation. We believe that our platform has the combination of features and value to our customers that will continue to allow us to compete favorably.

SALES & MARKETING

Our “land-and-expand” sales strategy focuses on acquiring new customers and building our existing customer relationships by using a direct-sales model. Over time, we expect our partners to include technology companies, consultants, service providers and accounting firms. We expect our partners to support our sales efforts through referrals and co-selling arrangements, as well as expand the use of MeasuredRisk through integrated technology offerings.

Our focus in to date has been in building and proving out our technology platform and service offerings and we have invested nominally into our sales and marketing efforts. Upon completion of the Offering contemplated herein, we intend to build human resources to launch customer success and professional services teams help our account managers build our existing customer relationships by providing advice and best practices that enable users to harness the full power of MeasuredRisk. We believe our sales strategies position us to build relationships over time as we add new users and solutions and expand to additional markets and geographies.

In addition, we intend to build a world-class marketing organization that will promote our brand, generate demand for our offerings and that will research and assess product and market needs. This will include an advance planning team to assess customer needs, conduct industry-based research and define new markets. And it will include a product marketing team to develop the go-to-market strategy for our platform as well as the applications built upon the platform and develops industry-level marketing messages. The product marketing team will also support our sales team with profiles of typical buyers, key messages, value propositions, competitive analysis and sales strategies.

We intend to develop and implement demand generation programs categorized by solution and industry, focused on engaging business leaders, process owners and technology teams. We will use a variety of marketing programs across traditional and social channels to target current and prospective customers, including:

- Using our website to engage and educate prospects on our platform and solutions.
- Employing search engine marketing and advertising, including search engine optimization and pay-per-click, to drive traffic to our website.
- Engaging customers and prospects through content marketing on social media, including Facebook, Twitter, LinkedIn and YouTube.
- Working with industry analysts to establish third-party validation and generate positive coverage for our platform and solutions.
- Sponsoring events and professional organizations.
- Producing webinars, workshops and customer meetings.
- Hosting an annual conference that brings customers together with our developers, professional services and customer success managers to learn and collaborate.
- Creating sales tools and field marketing events to support our sales organization to more effectively convert leads into customers.

RESEARCH & DEVELOPMENT

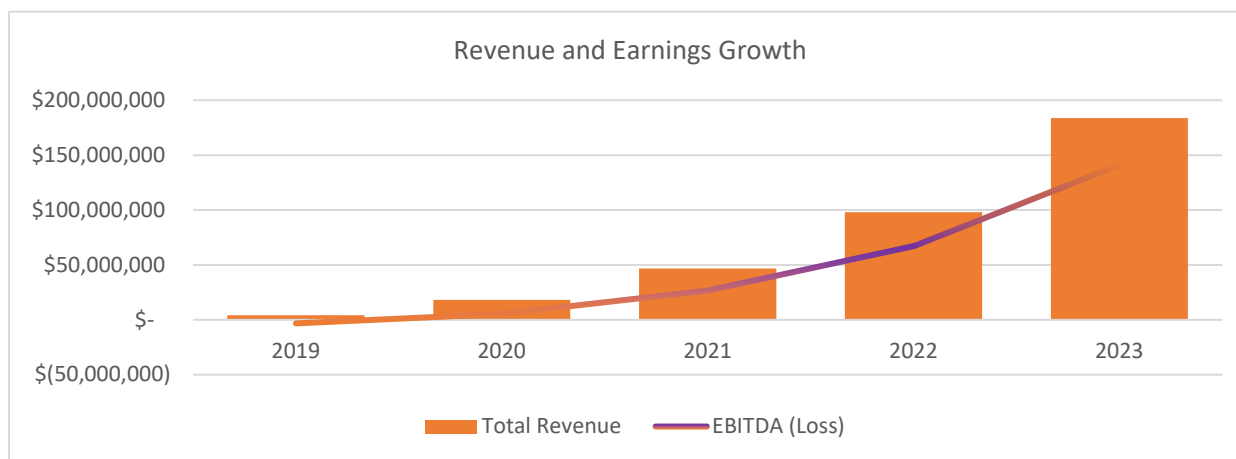
While our platform is fully developed and commercial-ready, we intend to continue to invest heavily into further research and development to ensure that we remain best-in-class and set standards, rather than follow them.

Our efforts are focused on improving the MeasuredRisk platform for broad use across all of our solutions. Our development teams can deploy incremental changes to our platform for our customers on a daily basis. We employ a continuous delivery process and a proprietary quality assurance process. We believe our focus on user experience and

our rigorous quality assurance culture are key differentiators that contribute to the success of our MeasuredRisk platform.

PRO FORMA FINANCIAL FORECAST ⁷

	2019	2020	2021	2022	2023
Total Revenue	\$ 4,220,000	\$ 18,040,000	\$ 46,640,000	\$ 98,080,000	\$ 183,660,000
Total Direct Costs	-	-	-	-	-
Gross Margin	4,220,000	18,040,000	46,640,000	98,080,000	183,660,000
Total Operating Expenses	7,470,000	12,820,000	20,030,000	31,070,000	42,500,000
Operating Income (Loss)	(3,260,000)	5,230,000	26,620,000	67,020,000	141,170,000
Total Other Income	30,000	30,000	130,000	450,000	1,180,000
Income Taxes	-	1,090,000	5,320,000	13,400,000	28,260,000
Net Income (Loss)	(3,230,000)	4,170,000	21,430,000	54,070,000	114,090,000
EBITDA (Loss)	\$ (3,260,000)	\$ 5,230,000	\$ 26,620,000	\$ 67,020,000	\$ 141,170,000
%	-77%	29%	57%	68%	77%
Total Current Assets	\$ 2,460,000	\$ 7,090,000	\$ 28,990,000	\$ 83,670,000	\$ 197,840,000
Fixed Assets, Net	-	-	-	-	-
Total Other Assets	-	-	-	-	-
Total Assets	2,460,000	7,090,000	28,990,000	83,670,000	197,840,000
Total Current Liabilities	680,000	1,150,000	1,630,000	2,240,000	2,330,000
Total Long-Term Liabilities	-	-	-	-	-
Total Equity	1,780,000	5,940,000	27,360,000	81,430,000	197,840,000
Total Liabilities and Equity	\$ 2,460,000	\$ 7,090,000	\$ 28,990,000	\$ 83,670,000	\$ 197,840,000
Total Cash From (For) Operating Activities	\$ (2,940,000)	\$ 3,520,000	\$ 19,520,000	\$ 50,390,000	\$ 107,050,000
Total Cash From (For) Investing Activities	-	-	-	-	-
Total Cash From (For) Financing Activities	5,000,000	-	-	-	-
Net Increase (Decrease) In Cash	2,070,000	3,520,000	19,520,000	50,390,000	107,050,000
Cash and Cash Equivalents-End	\$ 2,070,000	\$ 5,590,000	\$ 25,110,000	\$ 75,490,000	\$ 182,530,000
Enterprise Value Based Upon Multiple	\$ -	\$ 52,300,000	\$ 266,200,000	\$ 670,200,000	\$ 1,411,700,000
Total Equity Value (EV-LTD+Net Cash)	2,070,000	57,890,000	291,310,000	745,690,000	1,594,230,000



⁷ The projections herein assume, amongst other things, that the Company will complete its Offering contemplated herein on a timely basis. Failure to do so will cause a material adverse impact in these projections.

MANAGEMENT TEAM

Tom Albert, CEO and Founder. Tom is a transformative leader who has been bringing business relevance to IT and Security for over 17 years. A pioneer in creating highly differentiated solutions to protect information assets, he is known for identifying disruptive technologies and building innovation across the cyber landscape. Starting his career on Wall Street working with top global financial institutions, Tom transitioned to various leadership roles within Oracle, Symantec and Rainbow Technologies. Joining Cisco's team in 2007 Albert managed the National Security Operation, a \$320 million-dollar line of business within the U.S. Federal market segment and managed the U.S. Federal Civilian security business. He eventually became Cisco's Senior Advisor for cyber security and was instrumental in building their go-to-market strategy, solution portfolio, and crafting messaging frameworks which are still in use today. Tom also served as Vice President of Corporate & Business Development for Lancope where he worked on the creation of strategic partnerships spanning global markets; eventually identifying a route to market that drove massive growth resulting in the \$452M acquisition by Cisco in 2015. Building MeasuredRisk, Tom has redefined how business and government leaders see risk. MeasuredRisk has pioneered the Risk Inference market through the introduction of its flagship platform, View. Within one year of its founding, MeasuredRisk has been named one of the Top 10 cyber security companies in the world by several leading publications and industry analysts. — Tom's work as an industry expert and frequent speaker on the topic of cyber security spans major news networks and industry publications. Tom holds a B.A. from Pennsylvania State University.

Yuri Koshkin, Co-Founder. Dr. Koshkin brings approximately twenty years of advisory experience working with clients in Russia, Ukraine and throughout Eastern Europe and Central Asia. Prior to Measured Risk, following a career in the Former Soviet Union's military and intelligence communities he co-founded Trident Group in 1996. Under his leadership, Trident Group has advised many large US and global companies in a variety of key sectors, including energy, aerospace, telecommunications, investment and financial services, insurance and filmmaking and entertainment. Dr. Koshkin is a frequent commentator on major TV and radio networks and has been profiled in Businessweek and Portfolio magazines. He graduated from the Moscow Military Institute, Ministry of Defense. Dr. Koshkin received a PhD in History and International Relations from the Institute of the USA and Canada Studies, Russian Academy of Sciences in Moscow.

Tony Alagna, Chief Technology Officer. Tony Alagna is an early pioneer of disruptive cybersecurity technologies, having built platforms for anti-phishing and anti-malware that have been heavily utilized around the world. In the year 2000, Alagna founded WholeSecurity in his early twenties, raising over \$18.5M of venture capital into the company, captured the endpoint security market and eventually sold the company to Symantec when he was 27 years old. WholeSecurity was named one of Fortune's Top 25 Breakout Companies and was featured often in Forbes Magazine. Following WholeSecurity, Alagna continued to innovate while raising an additional \$35M to develop and support various business and philanthropic initiatives. Alagna holds an MBA from University of Texas.

For a complete list of MeasuredRisk management and advisory team see [About Us](#) at the Company's website.

DISCLAIMER

This is Not an Offer to Purchase or Sell Securities. This overview is for informational purposes and is not an offer to sell or a solicitation of an offer to buy any securities in the Company and may not be relied upon in connection with the purchase or sale of any security. Securities of the Company if offered, will only be available to parties who are "accredited investors" (as defined in Rule 501 promulgated pursuant to the Securities Act of 1933, as amended) and who are interested in investing in the Company on their own behalf. Any offering or solicitation will be made only to qualified prospective investors pursuant to a confidential offering memorandum, and the subscription documents, all of which should be read in their entirety.

To obtain further information, you must complete our investor questionnaire and meet the suitability standards required by law.

Cautionary Note Regarding Forward-Looking Statements/Pursuant to the U.S. Private Securities Litigation Reform Act of 1995

This investment brief contains, and our officers and representatives may from time to time make, "forward-looking statements" within the meaning of the safe harbor provisions of the U.S. Private Securities Litigation Reform Act of 1995. Forward-looking statements can be identified by words such as: "anticipate," "intend," "plan," "goal," "seek," "believe," "project," "estimate," "expect," "strategy," "future," "likely," "may," "should," "will" and similar references to future periods. Examples of forward-looking statements include, among others, statements we make regarding launch of products, sales, markets, marketing strategies, our estimates on future financial performance, revenue growth and earnings, anticipated levels of capital expenditures and our belief that offering proceeds will provide sufficient liquidity to fund our business operations over the next 36 months.

Forward-looking statements are neither historical facts nor assurances of future performance. Instead, they are based only on our current beliefs, expectations and assumptions regarding the future of our business, future plans and strategies, projections, anticipated events and trends, the economy and other future conditions. Because forward-looking statements relate to the future, they are subject to inherent uncertainties, risks and changes in circumstances that are difficult to predict and many of which are outside of our control. Our actual results and financial condition may differ materially from those indicated in the forward-looking statements. Therefore, you should not rely on any of these forward-looking statements. Important factors that could cause our actual results and financial condition to differ materially from those indicated in the forward-looking statements include, among others, the following:

Risks Related to the Company's Business

- *The Company has limited operating history, which makes it hard to evaluate its ability to generate revenue through operations.*
- *We have not been profitable historically and may not achieve or maintain profitability in the future.*
- *Failure to manage our growth may adversely affect our business or operations.*
- *Failure to manage our growth may adversely affect our business or operations.*
- *There is no assurance that the Company will be able to continue as a going concern.*
- *Our solutions face intense competition in the marketplace. If we are unable to compete effectively, our operating results could be adversely affected.*
- *Our revenue growth will depend in part on the success of our efforts to augment our direct-sales channels by developing relationships with third parties.*
- *Failure to establish and maintain relationships with partners that can provide complementary technology offerings and software integrations could limit our ability to grow our business.*
- *If we do not keep pace with technological changes, our solutions may become less competitive and our business may suffer.*

- *Any failure or interruptions in the internet infrastructure, bandwidth providers, data center providers, other third parties or our own systems for providing our solutions to customers could negatively impact our business.*
- *Any failure to offer high-quality technical support services may adversely affect our relationships with our customers and our financial results.*
- *We cannot accurately predict subscription renewal or upgrade rates and the impact these rates may have on our future revenue and operating results.*
- *We cannot accurately predict subscription renewal or upgrade rates and the impact these rates may have on our future revenue and operating results.*
- *We depend on our senior management team and other key employees, and the loss of one or more key employees could adversely affect our business.*
- *We depend on our senior management team and other key employees, and the loss of one or more key employees could adversely affect our business.*
- *Our workforce is our primary operating expense and subjects us to risks associated with increases in the cost of labor as a result of increased competition for employees, higher employee turnover rates and required wage increases and health benefit coverage, lawsuits or labor union activity.*
- *Our workforce is our primary operating expense and subjects us to risks associated with increases in the cost of labor as a result of increased competition for employees, higher employee turnover rates and required wage increases and health benefit coverage, lawsuits or labor union activity.*
- *The success of our platform largely depends on our ability to provide reliable solutions to our customers. If a customer were to experience a product defect, a disruption in its ability to use our solutions or a security flaw, demand for our solutions could be diminished, we could be subject to substantial liability and our business could suffer.*
- *We are subject to U.S. and foreign data privacy and protection laws and regulations as well as contractual privacy obligations, and our failure to comply could subject us to fines and damages and would harm our reputation and business.*
- *Assertions by third parties of infringement or other violations by us of their intellectual property rights could result in significant costs and harm our business and operating results.*
- *If we fail to continue to develop our brand, our business may suffer.*
- *We may need to raise additional capital, which may not be available to us.*
- *We may acquire other companies or technologies, which could divert our management's attention, result in additional dilution to our stockholders and otherwise disrupt our operations and adversely affect our operating results.*

Risks Related to the Offering

- *There are no assurances that the Company will successfully raise the funds required to successfully operate its business plan, expand its products, and accelerate its sales and marketing effort.*
- *The Company's management will have broad discretion over the use of the net proceeds from this Offering.*
- *Purchasers may lack information for monitoring their investment.*

For more information:

Thomas Carter
Deal Box, Inc.
email: thomas@dlbx.io