

Cyber Insurance Underwriting:

Fresh Approaches for Cyber Risk Evaluation

1. Introduction

In today's digital age, cybersecurity has become an increasingly pressing concern for businesses of all sizes. As cyber threats continue to evolve and proliferate, the need for cybersecurity insurance has never been greater. However, despite the growing demand for such insurance products, insurers face unique challenges when assessing the risks associated with potential clients.

Unlike traditional forms of insurance, where abundant historical data allows for reliable risk assessments, cybersecurity threats are constantly evolving. This dynamic nature of cyber risk presents a challenge for insurers attempting to accurately predict the likelihood and potential impact of a cyber incident. Compounding this "hacker problem" is the reality that a company's digital footprint is also continually changing, with new assets and services coming online, especially with the rapid adoption of cloud and SaaS services. Consequently, even the companies seeking insurance may not fully know all the assets they need to protect. This "unknown unknowns" challenge further complicates accurate risk assessments, as it's nearly impossible to assess the risks associated with what is not known.

Market Size: The global cyber insurance market was worth approximately \$13 billion in 2023, almost double the \$7 billion from 2020 (Security.org).

Growth Projections: Munich Re estimates that the global cyber insurance market will increase from \$14 billion in 2023 to around \$29 billion by 2027 (Munich Re).

Market Growth Predictions: Current predictions suggest that the global cyber insurance market will experience rapid growth over the next five years (Statista).

Market Growth Trend: The global cyber insurance market tripled in volume between 2017 and 2022, according to the Swiss Re Institute (Insurance Information Institute).

This whitepaper seeks to explore these challenges in greater detail and to provide insights into the difficulties faced by cybersecurity insurance carriers. By understanding the nuances of cyber risk and its assessment, we aim to foster a more informed conversation around cybersecurity insurance, enabling insurers to better serve their clients in this ever-changing threat landscape.

2. Traditional Assessment of Risk

Assessing risks is a key part of the underwriting process of any insurance product. With most products though, there are an abundance of tools and data sources available that give us a pretty good indication of the risks we are underwriting.

Auto Insurance benefits from available historic data from Motor Vehicle Records (MVRs), Vehicle history through Vehicle Identification Number (VIN), and drivers' Individual Credit Reports as a predictor of future insurance claims.

Much the same way, Homeowner's Insurance has access to home inspection reports and public records about the property, including previous claims, liens, or other legal issues.

Likewise, Life Insurance benefits from individual's medical exam, medical records and prescription history to identify potential health issues.

The above are just a few examples of how most insurance products have access to reliable historic data for underwriting. But, the same can not be said for Cyber Insurance.

3. Cybersecurity Risk Assessment Challenges

Cybersecurity underwriting is quite a bit more challenging. While there are several different sources of historical data about security incidents, including related losses, properly assessing future risks are made more difficult by a few aspects unique to cybersecurity.

The threats are not static.

Unlike the known and predictable threats associated with medical, auto, life and other areas, the threats in the cybersecurity arena are human. While past incidents can be used to predict certain types of risk, such as ransomware type attacks that follow a similar pattern, cybercriminals are always working on new ways to accomplish their goals.

In the cybersecurity world we refer to these methods as Tactics, Techniques & Procedures (TTPs) and they are quite dynamic.

According to a report by Risk Based Security, there were 36 billion records exposed through data breaches in the first three quarters of 2020 alone. This highlights the need for tools that can keep up with the rapidly changing threat landscape.

Many types of security incidents represent known attack vectors and low-hanging-fruit, a growing number of incidents are driven by an attacker's will to achieve an objective. These represent a challenge for the attacker and new TTPs may emerge from this challenge. These new TTPs might become tomorrow's well-known vectors, but today they represent a previously unknown risk.

Threats can be complex in nature.

Within the world of cybersecurity there are both easy-to-discover issues, such as an open port or an exposed service or a simple exploitable vulnerability but many risks are more complex in nature. These multi-stage complex threat vectors represent harder to identify risks.

A study by Ponemon Institute revealed that 60% of organizations had experienced a multi-stage cyberattack in the past year, emphasizing the need for tools that can identify complex attack vectors.

Sometimes a small risk can become a much larger risk when combined with other seemingly inconsequential risks in a kind of Rube-Goldberg-like breach.

The assets are always changing.

Cybersecurity risks come from various sources, but many are tied directly to what amount to vulnerable IT assets. Vulnerability management is a critical part of a robust cybersecurity program. Performing regular vulnerability assessments begins with knowing what assets are in the inventory.



Due to the ease at which new assets can be provisioned through such things as automation or even the simplicity of onboarding cloud-based SaaS applications and compounding by events such as merger and acquisitions, organizations struggle to maintain an accurate IT asset inventory and even for those that do, the vulnerability assessments lag very far behind so any risk assessment will also lag.

Attackers use automated tools to scour the internet for any vulnerable assets they can find. This unbiased searching will surface these unknown unknowns. To be clear, they are usually finding these assets randomly and not part of a targeted attack on a company, but a discovered vulnerable asset will pique the interest of an attacker and the results would be the same. A compromise.

A survey conducted by Rapid7 found that organizations often struggle to maintain accurate asset inventories, with 39% reporting difficulties in this area. This underscores the need for real-time asset monitoring.

According to Gartner, emerging risks can lead to unexpected financial, brand, and reputation impacts. To address this challenge, it's essential to employ tools that can uncover unknown risks.

There are unknown unknowns that cannot be assessed.

The ease at which new systems can be provisioned or connected to a corporate network, lead to shadow IT whereas systems are introduced while the IT staff is unaware.


The existence of these systems represents a certain degree of unknown unknowns and will fall outside any attempts to measure associated risks since they are by definition unknown. While some might assume that an asset unknown to the company will be equally unknown to an attacker, this is a falsity.

Lack of Universally Accepted Standards

The absence of universally accepted standards in cyber risk assessment can be illustrated by the varied approaches companies take to measure their cybersecurity posture. While some may use frameworks like NIST or ISO standards, others might rely on proprietary scoring systems or ad-hoc evaluations. This inconsistency was highlighted in a survey by the Ponemon Institute, which found lack of common standard for cybersecurity, making it difficult for insurers to uniformly assess and compare the risk profiles of different organizations.

4. Current Tools used for Evaluating Cyber Risk

Some of the current methods used to identify cybersecurity risks are listed below. Each tool has its pros and cons. There are also a few newer methods that have emerged in recent years that are defined below.



Questionnaires and surveys to gather information about a client's cybersecurity posture.

Penetration testing to simulate a cyberattack and identify vulnerabilities.

Analysis of previous cyber incidents in the industry to identify common risks.

Review of a client's cybersecurity policies and procedures.



Cybersecurity Risk Scoring:

These tools collect data from various sources, including threat intelligence feeds, public databases, and open-source information. They analyze this data to calculate a risk score, which helps organizations understand their overall cybersecurity risk and make informed decisions.

External Attack Surface Mapping:

These tools scan the internet for an organization's publicly exposed assets, such as IP addresses, domains, and web applications. By mapping the external attack surface, organizations can identify potential vulnerabilities and take appropriate measures to secure their assets.

Threat Intelligence:

These tools aggregate and analyze data from a variety of sources, including threat feeds, security research, and historical attack data. By providing insights into emerging threats and attack patterns, organizations can proactively adjust their defenses and prioritize responses based on the most relevant risks.

Dark Web Monitoring:

These tools continuously scan the dark web for mentions of an organization's sensitive data, including credentials, intellectual property, and customer information. By monitoring these hidden areas of the internet, organizations can detect potential breaches early and take steps to mitigate the impact before the exposed data is exploited.

A word about Open Source INTelligence (OSINT)

Cybersecurity risk scoring and External Attack Surface Mapping (EASM) solutions rely heavily on Open-Source Intelligence (OSINT) data. While OSINT offers valuable insights, it also presents some challenges due to its inherent limitations.

One major limitation of OSINT data is its tendency to be outdated and incomplete. This is primarily because OSINT relies on internet-wide scanning, which cannot scan every IP address continuously. As a result, scans are performed infrequently, leading to an outdated dataset. This can pose significant issues for organizations seeking to address dynamic changes in their cybersecurity risk landscape.

Another aspect to consider when evaluating OSINT data is its passive nature. While OSINT data may have been initially collected through active scanning, it becomes passive once incorporated into risk scoring and EASM solutions. This passivity contributes to the limitations previously mentioned, such as outdated information and false positives or negatives.

To address these issues, organizations may opt for active scanning on demand. Active scanning provides up-to-date, real-time data, enabling a more accurate assessment of the current risk landscape. By actively scanning a company's infrastructure, potential vulnerabilities and emerging risks can be identified with greater precision, effectively reducing false positives and false negatives.

According to research by the SANS Institute, false positives and negatives are common in vulnerability scanning tools, which can lead to wasted resources and increased risk exposure.

A report by Forrester Consulting found that organizations that implemented continuous monitoring saw a 92% reduction in the time required to detect and respond to security incidents.



While active scanning may require additional resources and expertise, the benefits of a more accurate and timely risk assessment can significantly outweigh the costs, ultimately enhancing an organization's overall cybersecurity posture.

5. Limitations of Current Tools against Key Challenges

1. Questionnaires and surveys

- Dynamic Threat Landscape: Limited effectiveness, as they rely on historical data and self-reporting.
- Complex Threat Vectors: Limited in capturing complex, multi-stage attacks.
- Rapidly Changing Assets: Limited in capturing real-time changes to assets.
- Unknown Unknowns: Can't capture unknown risks.

2. Penetration testing

- Dynamic Threat Landscape: Helpful in identifying current vulnerabilities but may not account for emerging TTPs.
- Complex Threat Vectors: Can identify individual vulnerabilities but might miss complex threat vectors.
- Rapidly Changing Assets: Snapshot-based, so it may not reflect the most current state of assets.
- Unknown Unknowns: Can identify some unknown risks but is limited to tested areas.

3. Analysis of past incidents

- Dynamic Threat Landscape: Can inform about common risks, but new threats may not be reflected in historical data.
- Complex Threat Vectors: Provides insight into complex attacks but may not predict future, unseen attacks.
- Rapidly Changing Assets: Offers little insight into risks from rapidly changing assets.
- Unknown Unknowns: Doesn't provide insight into unknown risks.

4. Review of policies and procedures

- Dynamic Threat Landscape: Assesses preparedness for known threats, but not necessarily for emerging ones.
- Complex Threat Vectors: Can reveal how well a company handles complex threats but can't predict new ones.
- Rapidly Changing Assets: Provides an understanding of how a company manages asset changes but can't predict unknown risks.
- Unknown Unknowns: Offers insight into how a company might handle unknown risks but can't predict them.

5. Cybersecurity Risk Scoring

- Dynamic Threat Landscape: Provides a broad view of the threat landscape but might not capture organization-specific risks.
- Complex Threat Vectors: Limited in identifying complex threats specific to an organization.
- Rapidly Changing Assets: May not reflect real-time changes in assets.
- Unknown Unknowns: Helps uncover some unknown risks but not all.

6. External Attack Surface Mapping

- Dynamic Threat Landscape: Identifies exposed assets but doesn't account for emerging TTPs.
- Complex Threat Vectors: Limited in identifying complex threats involving internal assets or non-technical risks.
- Rapidly Changing Assets: Useful for real-time mapping of external assets but doesn't cover internal assets.
- Unknown Unknowns: May reveal some unknown risks related to the external attack surface but not those related to internal assets or non-technical risks.



7. Threat Intelligence

- **Dynamic Threat Landscape:** While it offers valuable insights into emerging threats and conversations about the company, it may not fully address organization-specific risks such as specific vulnerabilities and issues.
- **Complex Threat Vectors:** Provides general information on complex threats, but it often lacks the granularity needed to identify specific, multi-stage attacks tailored to an organization.
- **Rapidly Changing Assets:** Typically focuses on organization threats and not built for asset/vulnerability discovery.
- **Unknown Unknowns:** Not built for asset/vulnerability discovery.

8. Dark Web Monitoring

- **Dynamic Threat Landscape:** Effective at identifying threats in obscure areas of the internet but will less likely surface specific security issues for the organization.
- **Complex Threat Vectors:** Not really built to look for threat vectors and TTPs. Rather it is built to look for threat actors who might be targeting the organization or reselling their data/IP.
- **Rapidly Changing Assets:** Not built for asset/vulnerability discovery.
- **Unknown Unknowns:** Not built for asset/vulnerability discovery.

6. A New Tool for Accurate Cyber Insurance Underwriting

To address the limitations of current tools for quantifying cybersecurity risk, a new solution has emerged: **CyberMindr**.

CyberMindr is a fully automated, cloud-based platform that maps and validates multi-stage attack vectors, providing insurance companies with a precise and efficient tool for assessing cybersecurity risks during the underwriting process.

Developed by a team of expert red teamers and bug bounty hunters, CyberMindr stands out by focusing on validated vulnerabilities and confirmed attack paths, ensuring that insurers base their assessments on reliable and actionable data.

According to Gartner, combining external and internal data sources can provide a more holistic view of an organization's risk profile, allowing for better-informed decision-making.

With over 15,000 live checks on discovered assets and continuous updates from new live check playbooks, **CyberMindr** stays ahead of emerging threats. The platform's intelligence gathering from monitoring 300+ hacker forums offers insights into attackers' latest Tactics, Techniques, and Procedures (TTPs), which are crucial for accurate risk evaluation. This approach allows insurers to prioritize risks effectively, enabling them to make informed underwriting decisions and offer competitive premiums based on real and current cyber threats.

CyberMindr is an award-winning, 100% automated, cloud-hosted solution that requires no agents or access permissions, providing an external view that mirrors a real hacker's perspective. It performs real-time monitoring and comprehensive threat exposure assessments with near-zero false positives, delivering a more accurate and efficient risk assessment process.

Unlike traditional ASM tools, CyberMindr conducts active scans on public-facing and discoverable assets, including websites, servers, and applications, identifying only exploitable and confirmed vulnerabilities and attack paths.

A study by IBM found that organizations that took a proactive approach to cybersecurity had a 58% lower cost of data breaches compared to organizations with a reactive approach.



This method eliminates outdated data and minimizes the risk of false positives, providing insurers with reliable data for underwriting.

Key features of CyberMindr include:

A proprietary prediction engine that identifies assets not available through any OSINT sources, enhancing the comprehensiveness of risk assessments.

A validation engine, based on patent-pending technology, that confirms assets without triggering defensive security mechanisms, ensuring stealth and accuracy.

A multi-stage attack engine, continuously updated with new live checks to reflect the latest and evolving TTPs, keeping insurers informed of current risks.

CyberMindr equips insurance companies with the tools to efficiently and accurately assess cybersecurity risks, enhancing the underwriting process and ensuring more precise policy pricing.

7. How CyberMindr Addresses Challenges in Cyber Risk Identification

The dynamic threat landscape

The CyberMindr solution is built on a dynamic knowledgebase of current and emerging TTPs. The knowledgebase stays current through the monitoring of hacker networks and discussion forums by a team of cybersecurity professionals including penetration testers. By keeping current with the evolving threat landscape, CyberMindr can identify risks associated with new threats as they emerge.

Threat complexity

The attacker TTP knowledgebase that is at the core of CyberMindr solution is integrated into the solution through the creation of a library of attack scripts. These scripts, which as of this time includes almost 16,000, can be automatically executed via a multi-stage-attack & validation engine.

Additionally, the granular nature of the attack script library allows these scripts to be strung together into complicated multi-step attacks which in turn facilitates the evaluation of more complex threats that lead to more obscure risks which are typically missed by other solutions.

Changing asset inventories

When CyberMindr performs its automated risk assessment of a target, it begins by attempting to identify all assets associated with the target company. This automated inventory follows a zero-knowledge, un-biased discovery approach. It does not rely on a target company supplying or even knowing what their assets are.

While other external solutions also attempt to discover assets, as indicated earlier, these solutions overwhelmingly rely of OSINT type data sources which are full of many inaccuracies due to infrequent and incomplete data gathering methods. The resultant inventories of these solutions are far from complete (the false-negative problem) and are also plagued with assets that are mis-attributed (false-positives) to the target company.

As part of the discovery process, the CyberMindr multi-stage-validation engine will clean the data so that only validated findings are surfaced. CyberMindr successfully addresses industry’s nagging problem of false-positives and false-negatives.



Unknown Unknowns

One of the benefits of CyberMindr's zero-knowledge, un-biased discovery approach to asset discovery is that it can discover those unknown unknowns. The first step of the asset discovery process involves casting a very wide net across many different data sources. While this approach is typically viewed as a negative because of all the errant data that is caught in that net, the CyberMindr validation engine can clean up this data as part of validation workflow that takes place before data is surfaced.

The CyberMindr solution also performs its own active scanning of assets to uncover additional information that can be used to improve the inventory when it comes to identification of software and services which is a critical step that needs to be completed before trying to evaluate risks associated with the assets.

Due to a very thorough understanding of how assets get provisioned as well as the typical types of errors made by the people who set them up, the CyberMindr solution performs additional discoveries via a predictive engine that is built into the discovery workflow.

Lack of standards

The CyberMindr solutions approaches risk evaluation by leveraging years of cybersecurity experiences that include a variety of best practices. These best practices span all areas of security as well as many different types of frameworks. While a uniform, universally accepted, set of standards do not exist, basic security concepts are represented across everything from NIST's Cyber Security Framework to the CIS Top 18 Critical Security Controls to the MITRE ATT&CK Framework. By evaluating assets against known security and individual product best practices, you are measuring risk in a way that crosses most security standards.

8. Conclusion

In the rapidly evolving landscape of cybersecurity, traditional risk assessment methods fall short in accurately predicting and managing the complex and dynamic nature of cyber threats. As this whitepaper has explored, the inherent challenges in assessing cybersecurity risks—such as the unpredictable tactics of cybercriminals, the ever-changing digital assets of organizations, and the unknown unknowns that elude standard evaluation—highlight the urgent need for more sophisticated tools and approaches.

The introduction of advanced solutions like CyberMindr marks a significant step forward in addressing these challenges. By offering real-time, validated insights into potential vulnerabilities and attack vectors, CyberMindr empowers insurers to make more informed underwriting decisions. This not only enhances the precision of risk assessments but also improves the efficiency of the underwriting process, enabling insurance companies to provide better coverage at competitive rates.

As cyber threats continue to grow in frequency and sophistication, the adoption of innovative tools like CyberMindr will be crucial for insurers seeking to stay ahead of the curve. By leveraging cutting-edge technology and continuously updating intelligence, CyberMindr provides a reliable and actionable framework for assessing cybersecurity risks, ultimately helping insurers protect their clients in an increasingly uncertain digital world.



9. About CyberMindr

CyberMindr was founded in 2021 by a team of security professionals who include experienced researchers, bug bounty hunters, penetration testers and red teamers.

It was built on the underlying principle that cybersecurity involves doing many little things, repeatedly, and at scale, all the while validated everything to allow security teams to focus on things that matter to the underlying security of the organization they are protecting.

CyberMindr's Successful Use-Cases:

- ✔ investment management companies (private equity, venture capital, Industrial groups) to help them have a robust control on their portfolio's security posture
- ✔ Insurance Underwriting, as the platform eliminates 'false positives' from the threat detection methods, and help underwriters have a real sense of risks they are underwriting; as well as have ways of evaluating emerging threats through the period of insurance cover.
- ✔ M&A due diligence to review cyber threats/exposure as a part of deal cycles
- ✔ Third-part cyber risk monitoring of vendors and partners connected to the organization network
- ✔ SaaS Healthscan as a security governance to enforce security guidelines on SaaS vendor, in view of the explosive SaaS adoption happening in organizations

CyberMindr's Industry-First Features:

- ✔ Ability to actively scan and provide a security snapshot of the organization within a few hours
- ✔ Ability to find assets outside of the typical OSINT based sources other solutions rely on
- ✔ Validate all assets and vulnerabilities to reduce the false-positives associated with most other solutions
- ✔ A consistently growing library of attacker TTPs, that evolve as new threats emerge, and hence help companies manage their Zero Day threats
- ✔ Remediation advice for discovered issues for quicker Remediation efforts

CyberMindr helps mitigate risks of Ransomware, Wire fraud, Data Breaches, as well as helps minimise downtime from the past, ongoing and likely future successful Cyber Attacks.

Outside of the platform, a variety of other security services are available.

24x7 fully managed SOC
Forensic Analysis

PenTesting
Incident Response

Red Teaming
Wirefraud Bootcamp

Cloud Security Audit
CyberSecurity Workshops

USA

161 Fort Evans Rd NE.,
Suite 235, Leesburg,
VA 20176

Email: info@cybermindr.com

UK

16 Upper Woburn Place,
London, WC1H 0AF,
United Kingdom

Japan

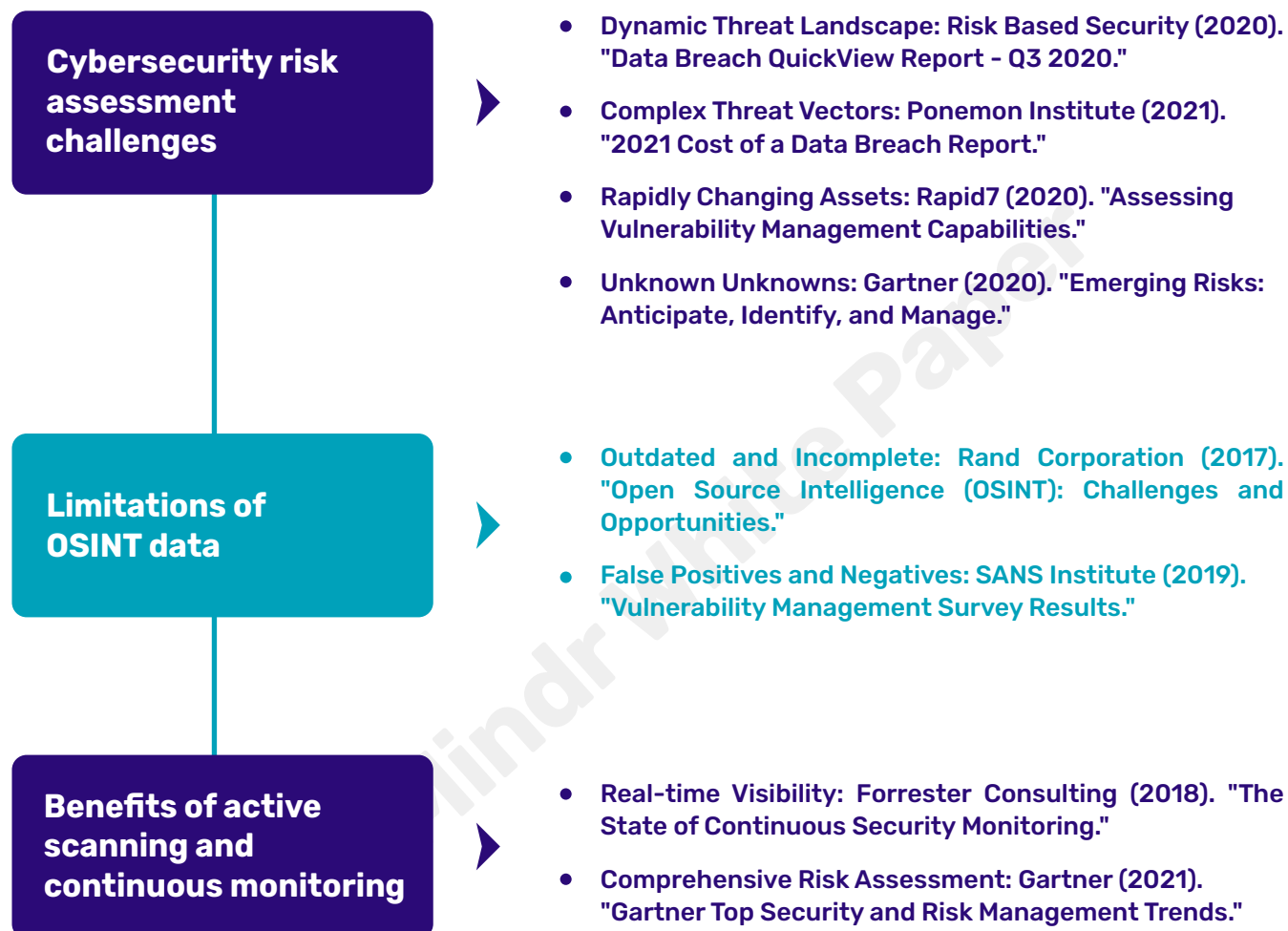
8F#B Otomo Bldg.,
1-5-18 Otsuka,
Bunkyo-KU, Tokyo

INDIA

652, 22nd Cross, 23rd
Main Rd, Parangi Palaya,
Sector 2, HSR Layout,
Bengaluru, Karnataka



10. References



USA

161 Fort Evans Rd NE.,
Suite 235, Leesburg,
VA 20176

Email: info@cybermindr.com

UK

16 Upper Woburn Place,
London, WC1H 0AF,
United Kingdom

Japan

8F#B Otomo Bldg.,
1-5-18 Otsuka,
Bunkyo-KU, Tokyo

INDIA

652, 22nd Cross, 23rd
Main Rd, Parangi Palaya,
Sector 2, HSR Layout,
Bengaluru, Karnataka

