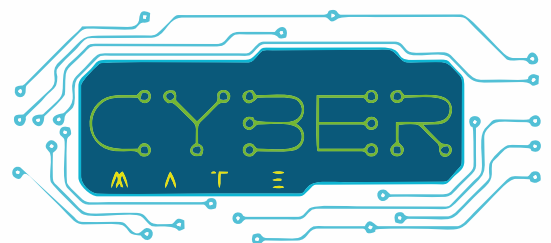




**CYBERMATE
FORENSICS & DATA SECURITY
SOLUTIONS PVT. LTD.**

Sec-U-ri-ty

"You" are at the center. Think about it.



Prepare & Prevent:

1. Information Security Audits:

Ensure that your third parties are handling sensitive data according to regulatory guidelines and industry standards with our cyber audits and reviews.

Your data. Their systems. Whose standards?

No matter how secure your company's IT system is, sometimes your risk of data breach depends on who you associate with. In today's complex business environment, large amounts of sensitive data are often shared with partners, outside vendors and service providers - who all have their own dedicated IT systems, processes and protections.

Cybermate's Third Party Reviews can help ensure that your business partners - or companies you refer your customers to - hold the same high standards you have when it comes to data security. Third Party Reviews are

especially important in highly regulated environments like healthcare, finance, or insurance - where data breaches are a costly and critical issue. Third Party reviews can also be important for companies working on critical infrastructure.

Before you put your reputation in someone else's hands, reach out to Cybermate's Third Party Reviews team. Our trained and licensed Third Party Review experts bring objectivity and quantifiable results - giving you the information you need to make sound business decisions.

2. Vulnerability Assessment:

We utilize vulnerability scanning software with the most up-to-date data security information that help our experts deliver actionable and prioritized recommendations to improve your IT security.

Vulnerability Assessment :

Vulnerability analysis, also known as vulnerability assessment, is a process that defines, identifies, and classifies the security holes (vulnerabilities) in a computer, network, or communications Infrastructure. In addition, vulnerability analysis can forecast the effectiveness of proposed countermeasures and evaluate their actual effectiveness after they are put into use.

Benefit from Vulnerability Assessment:

- Data protection and empowering businesses to better shield its systems from malicious attacks
- Reduce cost of security breaches
- Good reputation in front of clients, as your clients also want that their information stays protected.
- Concrete action plan based on the report to ensure security of existing and new technologies
- Management gets clear visual of security improvements with tracking

3. Penetration Testing:

Don't assume a crack is too small to be noticed, or too small to be exploited. If you do a penetration test of your network and 97 things pass the test but three esoteric things fail, don't think they don't matter.

Your organization's data and networks are under siege by cyber criminals. As a security-conscious organization, you continually try to protect against the many threats and vulnerabilities facing your cyber assets. How confident are you that your protective measures are effective against current and emerging cyberattacks?

Our penetration testing team assesses your company's information security through simulated attacks on your organization. Using real-world hacker techniques, we

identify gaps in your existing security. Common targets include the internet perimeter, internal and external network infrastructure, websites, databases, applications, and even your organization's employees.

At the conclusion of our penetration testing services, we provide substantive evidence of vulnerabilities and recommendations for effective countermeasures to reduce your risk. This allows your company to take action before a cyber intruder can compromise your system and steal sensitive and valuable data.

Investigations & Respond.



1. Cyber Crime Investigations:

Cybermate has the global expertise and resources necessary to investigate a range of cybercrime activity, employing a full range of investigative strategies to identify system vulnerabilities, intrusions and data ex-filtrations and to recommend appropriate and cost-effective solutions that can be applied across the enterprise.

We collect and examine physical and digital evidence to uncover important information about an incident to determine where and when an incident occurred, as well as how it happened. We can determine what data was compromised and whether digital evidence was erased or

modified, recover data, and recreate events and exchanges so that you have an accurate diagnosis to develop an effective recovery plan.

Cybermate offers a full range of investigative resources for an effective investigation of cybercrime, ranging from data collection and analysis to conducting fraud and internal investigations. We combine computer forensic expertise with traditional investigative methodology, including interviews and surveillance in order to retrace the behavior of people may have had access to protected or proprietary information.

2. Cyber Forensics:



Cybermate's computer forensics experts ensure that no digital evidence is overlooked and assist at any stage of an investigation or litigation, regardless of the number or location of data sources.

Claims of fraud, financial tampering, computer crime, employee misconduct, and other wrongdoing require corporations, law firms, and government agencies to follow digital trails to piece together facts that lead to the

truth. Cybermate's computer forensics experts help ensure no digital evidence is overlooked and assist at any stage of a digital forensics investigation or litigation, regardless of the number or location of data sources. Trust Cybermate computer forensics experts to assist you with your most complex and sensitive investigative or litigation matters involving electronic evidence or data preservation.





Allied Services :

1. Data Breach & Incident Response:

For peace of mind after a data breach, rely on Cybermate's rapid response team of cyber experts for compliant notifications; reputation-saving remediation; and litigation support.

Even with the most robust controls in place, a data breach may still occur.

Cybermate has helped countless organizations worldwide respond to data loss - and we can help you. We respond quickly when your confidential information is

compromised, no matter the source of the data breach, whether it's the result of a malicious hacker or a negligent employee.

Whatever your incident response challenges, we'll work with you to:

- Secure critical evidence to support investigation or litigation needs
- Defend against internal and external exposure
- Retain customers and opportunities
- Apply processes for future prevention

One choice ... total data breach response solution

As the leading provider of end-to-end cyber security, data breach response and incident analysis solutions, we offer expert guidance to improve your outcomes across the board. We'll help you make informed

decisions at every turn to guide you along a smooth path to recovery - one that leaves you standing in the best defensible position, reputation intact, where "business as usual" proceeds without disruption.

2. Training & Awareness Programs:

In awareness activities, the learner is the recipient of information, whereas the learner in a training environment has a more active role. Awareness relies on reaching broad audiences with attractive packaging techniques. Training is more formal, having a goal of building knowledge and skills to facilitate the job performance.

An example of a topic for an awareness session (or awareness material to be distributed) is virus protection. The subject can simply and briefly be addressed by describing what a virus is, what can happen if a virus infects a user's system, what the user should do to protect the system, and what the user should do if a virus is discovered.

“Training strives to produce relevant and needed security skills and competencies”.

We reckon our specialization with this kind of training. On-site training is provided in all the major sectors, where our team of trainers and specialized instructors

come down to your college, school, corporate or government office and impart you with technical know-how and skill sets.

IT Audits | Vulnerability Assessment | Penetration Testing | Cyber Crime Investigations | Cyber Forensics
Data Breach & Incident Response | Cyber Stalking / Harassment | Training & Awareness Programs.

Address: Chintamani, Sujay Garden, Mukundnagar, Pune - 411037, India.
Contact: +91 9921498309, +917350688009 | sales@cybermateforensics.com