SCAN TO READ THIS ARTICLE IN ENGLISH

SCAN TO READ THIS ARTICLE IN HINDI

Viral Shah

Bridging Cybersecurity, Digital Investigation, and Legal Evidence in the Modern Business Landscape

Kaushal Kumar | The CEO Magazine

Viral Shah
Cyber Security & Digital Forensic Expert

As businesses become increasingly dependent on digital systems, cyber incidents today extend far beyond technical disruptions. From insider threats and financial fraud to manipulated data and security breaches, organisations are facing growing pressure to not only respond to attacks but also determine exactly what happened and who was responsible. It is this growing need for credible digital investigation and evidence-based analysis that led Viral Shah to build his practice in cyber forensics.

Established in 2018, Viral Shah's Cyber Forensics Investigation has positioned itself as a specialised cyber forensics and digital evidence investigation agency serving law enforcement agencies, insurance companies, NBFCs, nationalised banks, corporations, and various courts and tribunals. With ISO 9001:2015 and ISO/IEC 27037:2012 certifications, the organisation focuses on bridging the gap between complex technical analysis and legally admissible evidence through a comprehensive approach that spans incident response, memory forensics, data recovery, and vulnerability assessments. Over the years, achieving ISO certifications, resolving more than 1,000 cases, and becoming a trusted partner for nationalised banks, NBFC, Insurance companies, courts, tribunals and law enforcement agencies across India have emerged as key milestones for the organisation.

Building a Practice Around the "Digital Truth"

For Mr. Shah, the journey into cyber forensics began with observing the rapid digitalisation of corporate and personal data and the corresponding rise in sophisticated cybercrime. What initially drew him to the field was the need to identify and establish the "digital truth" in complex disputes and investigations.
Over the years, his approach has evolved significantly alongside the changing threat landscape. What once revolved around conventional hard drive recovery has expanded into sophisticated network breach investigations, advanced memory forensics, and proactive threat intelligence capabilities. Today, the organisation leverages its proprietary "CyberToolkit" alongside continuously upgraded forensic methodologies to address sophisticated cyber threats. Some selective and important features of this toolkit have been made available freely on their website.
For Mr. Shah, digital forensics extends far beyond technical analysis alone. *"It is absolutely a combination of a technical science, a legal discipline, and an investigative art. It requires the rigorous technical science of data extraction, the investigative art of piecing together a timeline of events, and the strict legal discipline of maintaining a flawless chain of custody so the findings hold up under cross-examination in court,"* he says.

Addressing Modern Cyber Threats

The organisation's core services encompass computer, network, mobile, and digital media forensics alongside incident response and comprehensive data recovery solutions. A significant area of specialisation lies in producing legally sound commercial evidence through email header analysis, hash value verification, and authentication of communication protocols such as SPF, DKIM, and DMARC to trace the origins of digital correspondence.

Corporates approach the organisation during high-risk situations involving unauthorised data copying, insider threats, financial fraud, and digital evidence acquisition from seized devices. In such cases, maintaining an unbroken chain of custody becomes critical to ensuring that evidence remains admissible during legal proceedings. Alongside investigations, the organisation also works closely with clients to improve awareness around digital evidence, cyber risk, and forensic preparedness, particularly among businesses that continue to underestimate their exposure to cyber threats.

"A common myth is that once a file is deleted or a system is formatted, the data is gone forever. Another misconception is that only large enterprises are targeted by cyberattacks," explains Mr. Shah. The organisation helps clients understand how persistent digital footprints can be and why small-to-medium enterprises are often equally vulnerable to cyber threats due to weaker security frameworks.

As cyber incidents become more legally consequential, Mr. Shah believes organisations can no longer afford to overlook the importance of digital forensics in modern business environments. "I would say that a cyber incident is no longer a matter of 'if', but 'when'. When a dispute arises or a breach occurs, relying on assumptions will fail you in a courtroom or a boardroom. Digital forensics provides the undeniable, scientific truth required to protect your assets and your reputation," he says.

Evolving with the Threat Landscape

One of the biggest challenges facing digital forensic practitioners is the rapid evolution of encryption technologies and anti-forensic techniques deployed by cybercriminals. To address this, the organisation continues to invest heavily in continuous education, international compliance standards, and upgraded forensic capabilities aligned with ISO/IEC 27037:2012 guidelines.

At the same time, the broader cybersecurity ecosystem is also undergoing a strategic shift. Organisations are increasingly recognising that the financial and reputational consequences of cyber incidents can no longer be addressed through reactive approaches alone. As a result, proactive threat intelligence and routine vulnerability assessments are becoming critical operational priorities.

The organisation continues to adapt traditional investigative principles to modern cloud architecture and evolving cyber environments by incorporating remote forensics, advanced memory analysis, and specialised cloud extraction techniques that preserve evidence integrity without disrupting live environments. Technology, according to Mr. Viral Shah, is also reshaping investigative capabilities at scale.

"AI and machine learning allow us to sift through terabytes of raw data in a fraction of the time it used to take, identifying anomalies and malicious patterns almost instantly. Remote forensics also enables our team to contain breaches and secure volatile memory data for clients globally without the delay of physical travel," he says.

As cyberattacks continue evolving, the organisation is preparing for a future shaped by AI-driven threats, deepfakes, and IoT vulnerabilities by continuously strengthening its capabilities in network and memory forensics alongside advanced threat intelligence integration.

Cybersecurity as a Foundation for Business Continuity

For modern enterprises, cybersecurity is becoming inseparable from operational continuity and long-term organisational health. Alongside investigations, the organisation also conducts workshops and awareness sessions focused on breach response protocols, phishing awareness, and digital evidence preservation for businesses and institutions.

Mr. Viral Shah believes a secure digital infrastructure directly contributes to stakeholder trust, reputational strength, and sustainable business growth, making it essential for organisations to integrate cybersecurity into decision-making from the very beginning rather than treating it as a reactive function.

> "IF YOU ARE UNDERGOING DIGITAL TRANSFORMATION, IMPLEMENT 'SECURITY BY DESIGN' FROM DAY ONE RATHER THAN AS AN AFTERTHOUGHT. IN THE EVENT OF A BREACH, MY FOREMOST ADVICE IS: DO NOT ATTEMPT TO FIX OR INVESTIGATE IT INTERNALLY WITHOUT EXPERTISE. ISOLATE THE SYSTEM AND CALL FORENSIC EXPERTS IMMEDIATELY TO AVOID DESTROYING VOLATILE EVIDENCE," - VIRAL SHAH.

Leadership Mantra

As digital systems continue to expand across industries, the need for skilled cyberforensic professionals is expected to grow significantly over the coming decade. Advising aspiring professionals entering the field, Mr. Shah says, *"Build a rock-solid foundation in networking, operating systems, and legal compliance. Obtain recognised certifications, but more importantly, stay relentlessly curious. Cyber forensics is not a 9-to-5 job; it requires a mindset of continuous learning because the technology you defend against changes daily."*