CYBER SECURITY AND FORENSIC SERVICES DIVISION

Background

The evolving corporate landscape has increased the importance and complexity of IT Infrastructure. While it has served as a boon in bringing in efficiency and productivity as compared to a paperbound world, it has also increased the risk of vulnerability and fraud.

The digital technologies and the internet are indispensable tools in modern era of business and the corporates are trying to leverage the ever evolving opportunities of cyber space from automating basic internal processes to adopting cloud services. While the Corporate's journey of digital adoption continues to grow, one misstep in the digital life cycle has cascading effect of cyber fraud, data breaches, ransomware, downtime, civil litigation and loss of business reputation.

Cyber Security and Forensic Audit Services are necessary for all organisations from a small start up to a global conglomerate to secure the IT environment. The audit provides an overall assessment of companies' hardware, software, network security, data-centre, potential vulnerabilities and suggests measures to strengthen the companies IT Infrastructure.

Thus, a process of technical evaluation that assesses the current status of your systems, applications, and network to gauge its performance. The audit ensures all systems are running optimally as per your business needs.

Some Typical Cyber Frauds/Crimes Affecting Businesses:

- Hacking involving compromise of Organisation's Critical Servers

- Phishing and email spoofing attacks

- Denial-of-service-attack that renders the resources useless

- State funded cyber-attacks on key Organisations

- Competitor sponsored attacks to gather sensitive Company's Information

- Defacement of a Company's Corporate Website

- Identity theft

- Electronic money laundering/fund diversion

- Theft of Intellectual Property

As a response, V Sahai Tripathi & Co ('VST') has set up a *Cyber Security & Forensic Services Division* which provides preventive as well as Investigative Fraud and Cyber Crime Services for Public and Private Corporations, as well as small and medium-sized businesses. We work closely with business owners, executives, and legal counsel to provide clear answers in complex cases where every investigation is led by a fraud examiner. Our Forensic Services team identifies and deals with a wide range of financial crime, business misconduct and fact-finding approach.

Our Team

Our Cyber Security & Forensic Services Division has a growing team of Professionals, which includes Chartered Accountants, Engineers, MBAs, Research Analysts, Journalists, former law enforcement officials, to assist clients in complex areas of fraud investigation, anti-fraud advisory, network forensic services, data leak forensic services, dispute resolution advisory etc. Our team includes-

- Pic 1 – Vishwas Tripathi (FCA)
- Pic 2 – Colonel Inderjeet Singh (Cyber Security and Forensics Expert)
- Pic 3 – Divyanshi Agarwal (Cyber Security and Forensics Specialist)
- Pic 4 – Garima Tripathi (ACA)
- Pic 5 – Barun (ACA)
- Pic 6 – Mahima Tripathi (Audit Manager)

Brief Profile Of Our Team Members:

Vishwas Tripathi B Com (Hons), FCA

Mr. Vishwas Tripathi was enrolled with ICAI as a member in 1988. He has an experience of more than 32 years in the profession with a graduate degree in B Com (Hons) from Shri Ram College of Commerce and is a promoter partner in CA Firm (V. Sahai Tripathi and Co.). He has rich experience in various fields, such as Taxation Law, Company Law, Auditing, Corporate Finance liaison, Non Residents Exchange control regulations services relating to setting up of liaison/project office in India, etc. His core expertise lies in Financial Consultancy, Management consultancy, Corporate advisory, Taxation, Investment planning and business advisory services. Further, he served as Chairman, Board of Directors, United News of India (UNI) continuously from March 2013 to March 2021.

Colonel Inderjeet Singh

Colonel Inderjeet Singh has served in the Indian Defence Forces, is Alumnus of IIT Kharagpur and Symbiosis Institute of Management, Pune. He is an experienced Information Systems professional with experience of more than 29+ year across wide spectrum of areas spanning cyber security operations leadership and influencing policy level decisions in multiple organizations. Throughout his career, he has parlayed his extensive background in security and a deep knowledge to help organizations build and implement strategic cyber security solutions.

He has consistently delivered mission-critical results in the field of in Information Security Management, Cyber Security, Cyber Warfare and Cyber Risk Management. He is visionary for Start-Up Incubation, Entrepreneurship Development, Strategic Consulting and New Technology Evaluation for commercial viability. He is a Subject Matter Expert on latest innovative Technological domains and effectively managed mission critical projects. He has been consistently awarded while in Army and was awarded:

- Magnificent CIO of the Year "Award in year 2016
- Excellence Award" by International Police Commission (IPC) 2019
- Fifty Innovative Leaders Award 2020, Cyber Security Leadership Award 2020
- 30 most Influential Indian thought Leader in Blockchain 2021

Divyanshi Agarwal B. Tech

Ms Divyanshi Agarwal is B.Tech graduate in computer science with specialization in cybersecurity forensics. Through her curriculum she has gained in depth knowledge in the field of cybersecurity, and has a great knowledge of the current trends in the industry.

Garima Tripathi B Com (Hons), ACA

Ms Garima Tripathi was enrolled as a member with ICAI in 2017. She has experience in the field of Audit, Accounting, Internal Auditing, Banking, Book Keeping and Information System Audits along with Financial Due Diligence. Her specialization is handling clients with vast data sets involving complicated transactions. Her client expertise is in Service Industry and Manufacturing Industries including setting up of procedural and accounting manuals.

Barun Kumar B Com, ACA

Mr Barun Kumar was enrolled as a member with ICAI in 2017. He has over 4 years of professional experience in statutory and tax audits of clients from diversified industries including FMCG, ITES, healthcare, real estate, educational institutes, etc. His areas of specialization include Statutory and Tax Audits, Financial Reporting, Advisory services on Ind AS & IGAAP.
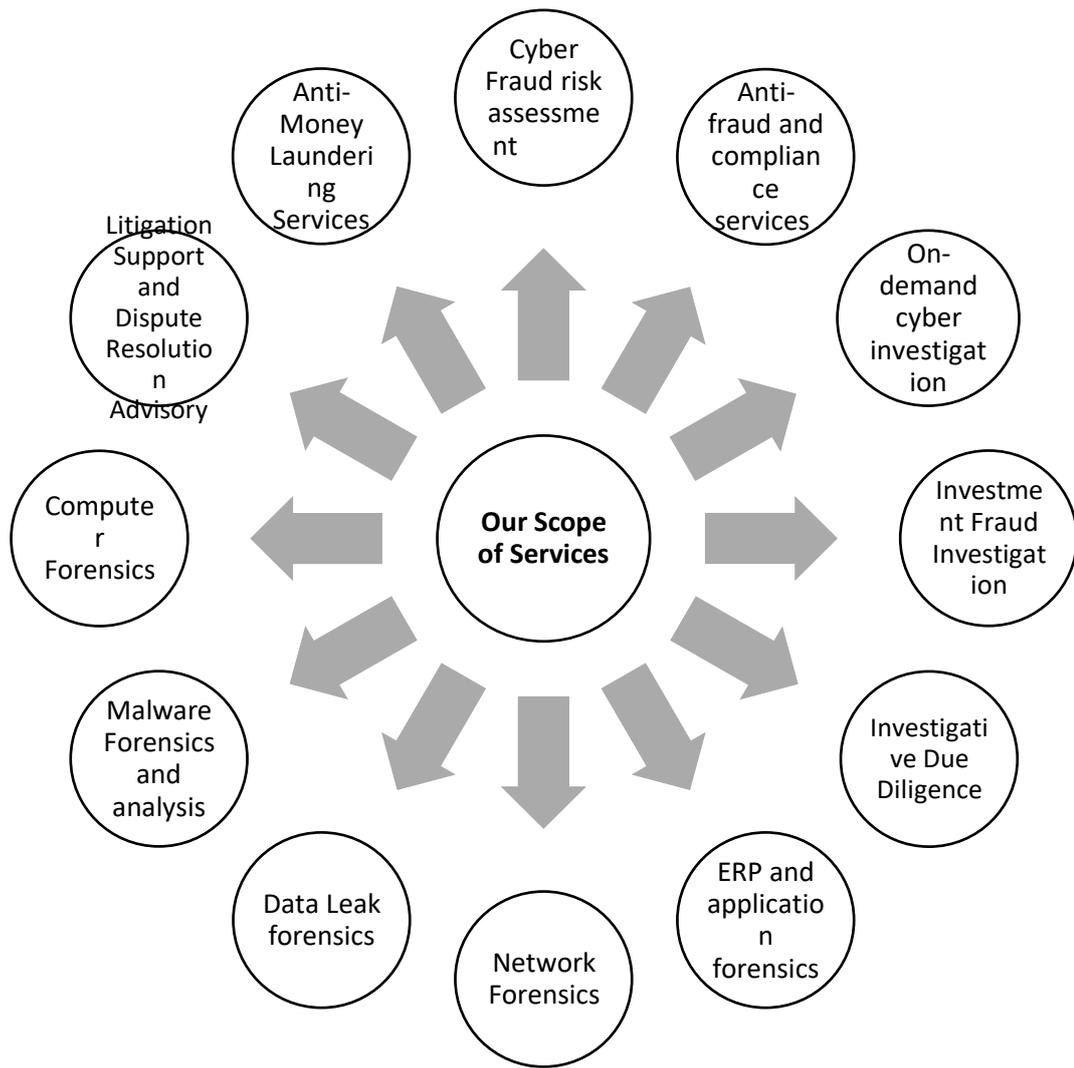
Mahima Tripathi B Com (Hons), Audit Manager

Ms Mahima Tripathi has completed her B Com (Hons) from Delhi University. She has experience in the field of Audit, Accounting, Internal Auditing, Banking and Book Keeping. Further she has completed her CA Training in Transfer Pricing from a reputed MNC and also having a good exposure in RBI and Other Regulatory Compliances required to comply by Non Banking Financial Companies.

Our Service Offerings

Our Cyber Security & Forensic Services Division practices a preventive and investigative approach in the analysis of transactions, books, records, testing of documents, conducting interviews, forensic data analytics, collecting market intelligence and evidence gathering using forensic technology tools that can provide cybercrime prevention opportunities and deep insight into fraud risks to the client.

A Snapshot Of The Services Provided By Us Is Given Below:

Our Scope of Services

- Cyber Fraud risk assessment
- Anti-Money Laundering Services
- Anti-fraud and compliance services
- On-demand cyber investigation
- Litigation Support and Dispute Resolution Advisory
- Investment Fraud Investigation
- Computer Forensics
- Investigative Due Diligence
- Malware Forensics and analysis
- ERP and application forensics
- Data Leak forensics
- Network Forensics

Detailed nature of the above-mentioned services provided by VST is shared below-

Cyber Fraud Risk Assessment

The complexity of IT Infrastructure within Corporates has made it necessary for Corporates to have an effective cyber fraud risk assessment strategy in place and have relevant systems and controls. Some of the critical questions being faced by most Board of Directors, CEOs, CIOs and CFOs today are:

- Is our data secure?
- Has some one stolen our critical data (financial, marketing, research, IP, customer data etc) despite having anti leak controls in place?
- Is someone reading our emails?
- Can our IT systems be compromised and brought down?
- Are our networks systems infected with malware?

VST's Cyber Security & Forensic Services Division can help clients assess their vulnerabilities to cyber fraud and define any weaknesses in their systems and help minimize their vulnerabilities to cyber fraud risks. VST's cyber fraud risk assessment solution is crafted to help clients in gauging how susceptible organisations are to cyber related threats. Our solution involves the following key assessment activities:

- ✓ Cyber Fraud Risk Assessment
- ✓ Cyber Controls Testing
- ✓ Vulnerability Assessment & Penetration Testing
- ✓ Cyber Red flag Analysis
- ✓ Cyber Resilience Testing

Anti-fraud and Compliance Services

VST's anti-fraud advisory services help clients in complying with the regulatory requirements, while creating awareness about these issues amongst their employees. Over time, this awareness can help employees deter possible incidents of fraud, misconduct, or non-compliance that they may be exposed to.

On-Demand Cyber Investigation Services

With the rise of cyber incidents and the complexity involved, the incident response has to be quick with subject matter experts involved. Businesses/Organisations lack the resources, skills and insights to effectively and timely respond to cyber-attacks. Having a strategic partner to provide subject matter expertise and skills is critical to address the concerns relating to Cyber Risk.

VST offers an on-demand cyber investigation team which can help to deliver the following solutions:

- ✓ Immediate access to subject matter expert (remotely or on ground) to be early responders for any cyber-event.
- ✓ Continued support for incident response and investigation at pre-agreed rates.

Investment Fraud Investigation Services

Investment fraud investigations are conducted for investors who suspect their funds may be at risk in an illegitimate or illegal offering and for victims seeking financial recovery from collapsed or corrupt schemes. The purpose of an investment fraud investigation is to determine what actually happened with the client's funds, who's responsible and to provide a clear reporting of the evidence to support a positive outcome in settlement demands, civil litigation and criminal prosecution. The investigation may also involve tracing and locating assets to assist fraud victims in securing financial restitution.

During a fraud examination, VST's investigators will gather and analyse the relevant facts of the investment scheme, identify the responsible parties and confirm their involvement through independent investigation, fact-finding and interviews. VST will also help client in documenting the extent of financial losses.

Investigative Due Diligence Services

Prior to any major business transactions, investigative due diligence is worthy of consideration.VST has ample resources and network to do a detailed verification, investigation, or audit of virtually every aspect of a company (or individual) for better decisions on joint venture, partnership, merger, acquisition and investments.VST can help clients to check the credit worthiness of a potential business partner or reputation check of the potential target, including their reputation among vendors, their payment schedule to vendors, and their salary schedule to employee and so on. Our expert team of investigators has the skills and necessary experience to uncover grave issues before the deal is done.

ERP and Application Forensic Services

With white collar crime on the rise, many CFO and CEOs are witnessing a multitude of frauds on ERPs and business applications, such as financial embezzlement/procurement frauds/sales fraud/payroll frauds/expense frauds/supply chain management and agency frauds.

With regard to the above, VST aims to provide the following solutions to the clients:

✓ Build fraud risk scenarios
✓ Review ERP and application configurations to test adequacy of fraud and cyber controls
✓ Execute fraud analytics on ERP/application data
✓ Validate/investigate key anomalies noted from results of fraud analytics

Network Forensic Services

Attacks on network infrastructure can take place from a multitude of sources, both external and internal. In many cases attacks succeed because of weaknesses in the elements such as traffic filtering on routers and firewalls, Rules on NIPS[1]/NIDS[2], Wireless network management, Network architecture etc.

---

[1]Network intrusion protection system
[2]Network intrusion detection system

With regard to same, VST aims to provide the following solutions to the clients:

- ✓ Incident investigation (if any required by client)
- ✓ Review of configuration on various network devices (firewall, router, IPS/IDS) to test adequacy of fraud and cyber controls
- ✓ Execute red flag analytics on key device log files to identify potential incidents
- ✓ Validate/investigate key anomalies noted from results of analytics

Data Leak Forensic Services

Cyber attackers target organisations for their most valuable asset i.e. data. The nature of the attack depends on the data targeted like Intellectual property, personally identifiable information, customer data and credit card data, financial/sales/production data, business plans, documents, agreements, emails, financial data etc.

VST has a team of experts who can help clients by conducting data breach incident investigations and review the configuration on IT elements concerning data handling (i.e. data base servers, shared platforms, folders, file transfer protocol, file servers, backup data) to test adequacy of privacy and cyber controls.

Malware Forensic services

Malware seems to be the new attack vehicle in cyber war and can be developed for all sorts of platforms and operating systems. Malware developers are also increasingly focussing on mobile devices. Malware is being used to launch a series of cyber-attacks such as data stealing, outage of infrastructure, cyber spying, data corruption, ransom threats etc.

VST's malware forensic services will help clients in investigating malware infection cases and suggest containment strategies. Our services include malware review to understand malware behaviour and review of configuration on various IT elements (Anti-virus servers, Anti-SPAM filters, Intrusion prevention system) to test adequacy of forensic and cyber controls and Malware attack simulation.

Computer Forensic services

It takes special skills, techniques and technology to find, gather and preserve digital evidence. Without rigorous data capture and discovery techniques, crucial evidence could be lost or may be dismissed by prosecutors and judges in a potential litigation.

VST has a team of specialists that can help in the identification, collection and forensic analysis of electronic data by doing the following services:

- ✓ Computer Incident Response
- ✓ Electronic data recovery
- ✓ IT Investigations
- ✓ Incident response program development
- ✓ Rapid Response Retainer

Litigation Support and Dispute Resolution Advisory

The rapid pace and complex manner in which commercial transactions between corporates are conducted has resulted in a large amount of litigation and disputes. To overcome such issues, experienced litigators require the support of dispute consulting professionals who can provide valuable financial insight and identify relevant risks.

VST's litigation and dispute resolution services provide critical support to businesses involved in complex disputes. Whether client's dispute involves lost profits, reasonable royalties, economic damages or business valuation, our litigation support and dispute resolution advisory team has the skills and experience to calculate the damages and carefully assess how the issue affects the business. In each engagement, we deliver deep financial insight and detailed case analysis to bolster client's legal position in any dispute.

Anti-Money Laundering Services

VST can help clients to understand and address their anti-money laundering ('AML') challenges with proven experience, solutions and results. Our multi-phased approach includes AML risk assessment, evaluation of AML/ KYC procedures and enhancement, training and awareness, compliance and internal control assessments.

AML programmes need to adapt to change as financial institutions grow. VST can help to identify gaps that will need to be filled by conducting an assessment of client's AML programme in its current state and comparing it to the AML programme that client's future state will require.
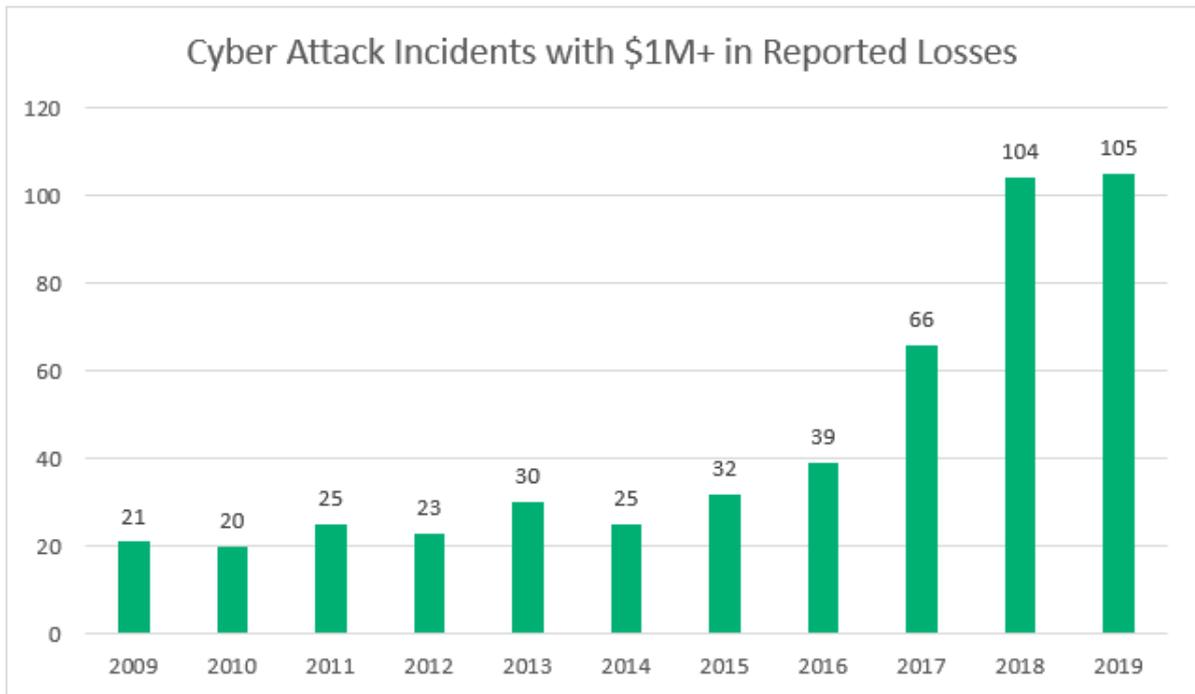
Risk Mitigation Measures

VST help clients to use the security policies in optimised manner to enhance the overall security and reduce the overall threat on the organisation whether it be the IT or physical threat. We will guide you through various prevention, deletion and remediation techniques to adapt and maintain an upper hand in security. This service will include a detailed guide through the 6-risk mitigation strategies:

- Conduct a risk assessment to determine vulnerabilities
- Establish network access controls
- Implement firewalls and antivirus software
- Create a patch management schedule
- Continuously monitor network traffic
- Build an incident response plan

Build Security Architecture For The Client

VST help client to provide overall solution of cyber security by providing it with a full threat proof personalised architecture that will act as a barrier to various threat keeping in mind the latest vulnerabilities of the time. This architecture will work as a foundation towards the building of security measures that are taken to avoid any sort of vulnerabilities. This will help as a great kick start for setting up a new organisation.

Graph Showing the Increase In Cyber-Attacks in Last more than one Decade

Cyber Attack Incidents with $1M+ in Reported Losses

Percentage of Different Types Of Attacks

Percentage of claims by attack technique

54% Email/phishing

29% Remote access

3% 3rd Party compromise

6% Other social engineering

3% Brute force (authentication)

3% Other