Data Security Practices

IT, including the Internet, occupies increasingly central role in fulfilling organizational mission in the globalized information economy. Buying of goods or services, transferring of funds through banks, making of credit card payments, sending of an email, interfacing with people through social networking sites, exchanging of pictures, videos or music are some of the activities that are routinely carried through the cyberspace. It is not only businesses that are critically dependent on the Internet, but also governments that are using e-governance applications to reach out to citizens for delivering services to them. Unfortunately, systems, networks and applications have vulnerabilities, which can be exploited by anyone connected to the Internet, to launch attacks against various targets such as corporate or government systems. Criminals can carry out identity theft and financial frauds; steal corporate information such as intellectual property; conduct espionage to steal state and military secrets; and recruit criminals and terrorists. Cyber attackers can disrupt critical infrastructures such as financial, power and air traffic control systems, which can result in outcomes, similar to those that maybe achieved by physical attacks by enemies or terrorists.

Insider threat being one among the top ten threats an organization faces, data loss prevention mechanisms play a key role in protecting the data within an organization. With all the avenues available to employees today to electronically expose sensitive data, the scope of the data loss problem is an order of magnitude greater than threat protection from outsiders.

The data loss vectors include:

- Data in motion – Any data that is moving through the network to the outside via the Internet.
- Data at rest – Data that resides in files systems, databases and other storage methods.
- Data at the endpoint – Data at the endpoints of the network (e .g . data on USB devices, external drives, MP3 players, laptops, and other highly-mobile devices).

DATA SECURITY POLICIES

Malav C. Sheth & Co., have in place reasonable commercial standards of technology and operational security designed to protect all information provided by visitors from unauthorized third party access. Remote Servers, emails and the internet are shaping the way financial service providers transact business. But the gains of the electronic age have come at the cost of financial data security breaches and cyber crime which directly impact the bottom lines and goodwill of financial organizations.

Instances of identity theft, phishing and fraud have left many financial organizations open to bad press, loss of revenues and law suits worth millions followed by the inevitable tumble at the stock markets causing immeasurable loss in investor confidence. Countries like the U.S. and UK

have enacted new financial data disclosure legislations to counter the rising incidence of cyber crime and to ensure improved financial IT security.

FINANCIAL DATA SECURITY

A recent study conducted on financial data security policies of global service providers concluded that most such organizations have data security measures that work only in reactive mode. That is, they kick start after lapses in financial data security are detected. Malav C. Sheth & Co., team of IT security experts made sure that we are ahead of the times in this respect.

Our financial data security policies work in a proactive 3-step process of prevention, detection and rapid response to deter potential network misuse or financial data security lapses. The experts at Malav C. Sheth & Co. have put in place high security financial service centers and surveillance systems that encompass all aspects of our clients' business: the people, processes and technologies within the organization including all third-party vendors outside it. Malav C. Sheth & Co. systems are devoid of external drives to avoid data duplication or copying and have restricted print permissions to prevent data misuse.

Our clients can be confident that Malav C. Sheth & Co. financial service delivery works on completely locked down system channels with financial data privacy measures that are secured through the utmost redundancy.

OUR PRIORITY TO DATA SECURITY

We respect our clients business and we give superior importance to the client data. We are committed to total integrity and confidentiality of customer information and have a comprehensive Security Policy to provide complete reassurance to our customers in this our services area of taxation & consultancy services. We have up to date training mechanisms to teach Tax preparers the need of data security. We are proud to say that all of our employees are trained in basic internet security measures.

We work to protect the security of your information during transmission through the software, which encrypts information you input. We constantly re-evaluate our privacy and security policies and adapt them as necessary to deal with new challenges. We do not and will not sell or rent your personal information to anyone, for any reason, at any time, unless it is in (i) in response to a valid legal request by a law enforcement officer or government agency or (ii) when you have explicitly or implicitly given your consent, or (iii). Utilize the same for some statistical or other representation without disclosing personal data.

We only reveal those numbers of your account as required to enable us to access and provide you the required services relating to your accounts. We make every effort to allow you to retain the anonymity of your personal identity and you are free to choose a Login ID email address and password that keeps your personal identity anonymous. Access to Your Registration Information and your personal financial data is strictly restricted to those of our Company employees and contractors, strictly on a need to know basis, in order to operate, develop or improve the Service. These employees or contractors may be subject to discipline, including termination and criminal prosecution, if they fail to meet these obligations. With the exception of a Login ID in the form of an email address, which may be provided on an anonymous basis, and your Third Party Account Information, which is required for providing the services, the Company does not require any information from you that might constitute personally identifiable information. It is important for you to protect against unauthorized access to your password and to your computer. Be sure to sign off when finished using a shared computer.

We understand that the security of the data of the clients stands as prime importance for them. Security policies have been put in place to ensure confidentiality of data at all levels. Some of our Features are

PHYSICAL AND WORK FLOOR SECURITY/ACCESS SECURITY:

- There is no printing, fax, or email facility to ensure that no sensitive data leaves the facility. Also, the employees get checked while entering and leaving the office premises.
- Screening of visitors/employees by a security guard during entry and exit for data storage media like CD 's.
- USB drives and CD's are banned from work-floor.
- The systems which processors use do not have CD drives and USB drive slots. All systems used in processing are denied email and web access. All systems are secured by anti-virus software that is regularly updated.
- Access Control lists – access logs are maintained and monitored.
- Non-disclosure Agreements with all employees.
- Each team member is provided with exclusive access rights to the data through individual domain accounts. The access rights are segregated as per the hierarchy level defined for a particular process. The respective member can access his part of source information only.

PROCESS FEATURES

- Non-disclosure / confidentiality agreements
- Audit trails for all system activities
- Access to registered and authorized users only
- Scanning of servers for penetration testing
- Large budget outlays on security

NETWORK SECURITY

- Use of secured line (128 bit SSL) to access and transmit data (images) from servers located in remote locations.
- Segmented LAN with firewall protection.
- All ports except DNS and SMTP servers are disabled for the external world.
- Security at both machine and network levels.
- Point-to-point data links.
- Virtual Private Network (VPN) protection and Secure Network
- Secure network firewalls
- Technology-driven detections systems
- Secure Encrypted Web Servers and laptops
- Password protected systems
- Biometric Access

ENTERPRISE ACCESS SYSTEM FOR EMPLOYEE LOGIN AND PC SECURITY

- Network and Windows Login
- PC 'locking'
- Secure Remote Access (VPN)
- Secure email
- Single sign on to enterprise and desktop applications
- Access to source documents is restricted to authorized employees only.
- Firewalls.
- Internet Security Training.
- No fax and printing capabilities at the processing site.
- PCs used by processors do not have CD ROM drives.
- PCs used in processing are denied web access.
- Limited usage of paper in the work-floor.
- In order to be host country law compliant, we ensure that there is no movement of data from the servers and the processed data is archived on those servers

Malav C. Sheth & Co. has also focused on financial IT security policies which have administrative auditing, reporting, and monitoring facilities that guarantee financial data security at every stage. Besides, Malav C. Sheth & Co. IT infrastructure has routine security features such as virus prevention/cure, spam filers and URL filtering. Workstations are secured individually by anti-virus protection and back-up drive manager.

Despite investments in state-of-the-art financial security devices and systems, our team of information security experts recognizes that the essential agents of security best practices are the individuals who man these work stations.

We undertake training reinforcement from time to time to sensitize employees and third party service providers on financial data privacy needs of our clients and on financial data security practices.

Please contact us for further information about Malav C. Sheth & Co. Services.