IMPLEMENTATION OF INFORMATION TECHNOLOGY ACT, 2000 AND THE MEASURES RECOMMENDED FOR BUSINESS MANAGERS

Written by ***Parag Kulkarni* & Rajlaxmi Wagh*****

** Government Class One Gazetted Officer and Student of Masters in Business Administration*

*** B.Com NIIT, LLM, Ph.D*

ABSTRACT

Though Computer Science is a blessing to mankind, even this field of Technology has not been spared of unfair exploitation. Unprecedented rise in use of the Infinite Cyber Space corresponding to the unimaginably rapid development of Information Technology is common knowledge. To Arrest Cyber Crime, the Information Technology Act was brought into force in our country. The Act is of Vital Significance to all the Students of Management because as Potential Managers, the students would not only be responsible for protecting themselves as well as other employees from Cyber Crime but also for preventing Members of their Organisation from being Penalised by Law. Managers today are confronted with the Dual Challenge of avoiding both, the commission of crime and omission of measures to fix responsibility. [1]

Towards that end, this Article would benefit the readers as under :-

(a) Raise the awareness level for Law for those who are already well versed with Information Technology.

(b) Improve the understanding of Cyber Security for those who are in the know of Legal Aspects.

(c) Refresh all Readers with Legal Provisions and Implementation Aspects of Cyber Security.

Although, Readers may not be new to Information Technology Act, this Article is unique; as it closely relates Provisions of the Act to the Practical Measures it elucidates, that can be derived for Implementation of the Provisions.

---

[1]. Dr. Rajlakshmi Wagh, 'TECHNOLOGICAL PROGRESS IN BRANDING – A CASE STUDY AND CYBER MANAGEMENT', International Journal of Advance Research - IJOAR.org ISSN 2320 – 91271 © 2014 Volume 2, Issue 5 of May 2014, Online : @ http://www.ijoar.org

Introduction to Information Technology Act

There can be no denying that Information Technology is the **world's fastest growing Technology**. Such growth is primarily attributable to exploitation of Information Technology in Business. While on the one hand, it has become **inescapable for a Business Manager** to be involved neck deep in utilizing Information Technology, he is always haunted by Cyber Crime on the other. **Importance of the Act can be gauged by the very fact that it amended various Sections of Indian Penal Code, 1860, Indian Evidence Act, 1872, Banker's Book Evidence Act, 1891, and Reserve Bank of India Act, 1934**. [2]

To Arrest the growing Cyber Crime, the Government of India brought the Information Security Act into force. The Bill declaring it as Law was passed in the Budget Session of 2000 and signed by President K. R. Narayanan on 09 May 2000. The bill was finalised by group of officials headed by then Honourable Minister of Information Technology Shree PramodMahajan. [2] A major amendment was made in 2008. It amended Section 66 (i.e. 66A), which Penalized sending of 'Grossly Offensive Messages'. It also introduced the Section 69, which gave authorities the power of 'Interception or Monitoring or Decryption of any Information through any Computer Resource'. It also introduced penalties for child pornography, Cyber Terrorism and Voyeurism. This amended Act was passed on 22 December 2008 without any debate in LokSabha. The next day it was passed by the RajyaSabha. It was signed by the then Hon. President Shreemati Pratibha Patil, on 05 February 2009. [3]

Relevance to Business Managers

Section 2 (i) of the Act defines a **'person' subject to this Act** as an individual; or a company or association orbody of individuals; whether incorporated or not; or Central Government or aState Government or any of the Ministries or Departments, Agencies orAuthorities of such Governments and Section 2 (l) defines a **'trusted person'** as any person who hasdirect responsibilities for the day-to-day operations, security and performance of Business Activities.[3] The laws apply to the whole of India. Persons of other nationalities can also be indicted under the law, if the crime involves a computer or network located in India. In short **all Business Managers** would invariably be governed by the Act. Besides Defining Cyber Crimes, the Act also prescribes penalties for them. Safeguards against Cyber Crimes is just one side of the Coin; the other being, Liability of Business Managers to the Act. [4]

Objectives of the Article

Objectives of this Article are as under :-

(1) To alert Business Managers about **exploitation by Cyber Criminals** for evading Penalties.

(2) To elucidate **Offences under Information Technology Act and Penalties.**

---

2. Wikipedia
3. Ministry of Information Technology, Government of India Notification dated 17 October 2000.
4. Section 1, Part 2 of the Gazette of India No 13 dated 05 Feb 2009**.**

(3) To give Practical Guidelines to Business Managers for prevention of Cyber Crime under their Jurisdiction.

(4) To recommend guidelines for System **Settings** Implementation.

Scope of Study

Scope of Study for this Article encompasses the following :-

(1) Determine vulnerabilities of Business Managers to Offences under the Act.

(2) Study Case Laws and Cite the same.

(3) Formulate Guidelines for preventing Cyber Crime.

(4) Determine System Settings.

Exploitation of Loop Holes in Business Management by Cyber Criminals

Expert Cyber Criminals are exploiting System Vulnerabilities to evade Cyber Security Laws by Hacking into the Computer System utilized by others and attacking the Targeted Systems through the Compramised System thereby making it almost impossible for Law Enforcement to identify the actual criminal. User of the Compramised Computer, would however get caught and Penalized. Therefore, in case Business Managers fail to implement adequate security measures, they will certainly remain vulnerable to **get roped in Cyber Crime** and face Penalties themselves.

Business Managers can fall prey to exploitation by any of the following methods adopted by Cyber Criminals [5] :-

(1) Click Jacking. Concealing Hyperlinks beneath Legitimate Action Buttons or Clickable Content which when clicked makes the User unknowingly perform illegitimate actions on behalf of the Cyber Criminal.

(2) Cross Site Scripting. Injection of Malicious Content into a Trusted Website Link or Web Address.

(3) Doxing. Releasing the Targeted Person's Identifying Information gathered through Social Networking.

(4) Pharming. Redirecting users from Legitimate Web Sites to Fraudulent ones to get such Acts carried out as the Cyber Criminals would not like to undertake by themselves.

(5) Phishing. Dropping an email impersonating a Legitimate Organisation or Person but actually containing a Link or Malware to be executed on behalf of the Cyber Criminal.

(6) Spoofing. Deceiving Computers or Users by hiding or faking Identity. [6]

Intimate Exploitation. No Cyber Criminal will, but obviously, ever reveal his identity as such; even if he is present in the near vicinity of the Computer belonging to some other User through which to commit Cyber Crime. Rather, **accessing the Computer belonging to another**

---

5. Information Technology Act 2000

6. Page 11, Unit 1 on Introduction to Cyber Security of 'Cyber Security, the only Solution to Safer and Effective Business', Published by IMED and Intelligence Quotient Systems Private Limited as Text Book for Certificate Course in Cyber Security,by Bharati

User would be the most Technically convenient method of preventing his own identity to surface. Therefore, the threat of a Business Manager's Computer being accessed by a Cyber Criminal as follows should not be underestimated :-

(1) When the Legitimate User is absent.

(2) When the Computer is unattended.

(3) Using the Computer for Cyber Crime by pretending to carry out tasks on behalf of the Legitimate User.

Protecting the Business Environment. Besides safeguarding themselves against exploitation in person, Business Managers will have to ensure that all Employees under their jurisdiction and their colleagues as well as Business Partners stay well protected in order to be effective. Good Business Managers would also be expected to advice their Superiors regarding enforcing implementation.

Offences and Penalties

A Business Manager is expected to take the whole Business Environment on to the path of growth. Cyber Crimes in the Business Environment are obviously detrimental to growth because of the **Penalties that such crimes invite and cause damage to Reputation as well as Goodwill** that the Business suffers. Therefore, it is essential for a Business Manager to be aware of the Offences under the Information Technology Act and Penalties. The Offences and corresponding Penalties have been summarized below :-

Section	Offence	Description	Penalty
66 A	Publishing offensive, false or threatening information	Any person who sends by any means of a computer resource any information that is grossly offensive or has a menacing character; or any information which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult shall be punishable with imprisonment for a term which may extend to three years and with fine.	Imprisonment up to three years, with fine.
65	Tampering with Computer Source Documents	If a person knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy or alter any computer source code used for a computer, computer programme, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force.	Imprisonment up to three years, or/and with fine up to ₹ 2,00,000

Section	Offence	Description	Penalty
66	Hacking with Computer System	If a person with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hack.	Imprisonment up to three years, or/and with fine up to ₹ 5,00,000
66 B	Receiving stolen computer or communication device	A person receives or retains a computer resource or communication device which is known to be stolen or the person has reason to believe is stolen.	Imprisonment up to three years, or/and with fine up to ₹ 1,00,000
66 C	Using Password of another person	A person fradulently uses the password, digital signature or other unique identification of another person.	Imprisonment up to three years, or/and with fine up to ₹ 1,00,000
66 D	Cheating using Computer Resource	If a person cheats someone using a Computer Resource or communication.	Imprisonment up to three years, or/and with fine up to ₹ 1,00,000
66 E	Publishing Private Images of others	If a person captures, transmits or publishes images of a person's private parts without his/her consent or knowledge.	Imprisonment up to three years, or/and with fine up to ₹ 2,00,000
66 F	Acts of Cyber-terrorism	If a person denies access to anauthorised personnel to a computer resource, accesses a protected system or introduces contaminant into a system, with the intention of threatening the unity, integrity, sovereignty or security of India, then he commits Cyberterrorism.	Imprisonment up to life.

Section	Offence	Description	Penalty
67	Publishing information which is obscene in electronic form.	If a person publishes or transmits or causes to be published in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it.	Imprisonment up to five years, or/and with fine up to ₹ 10,00,000
67 C	Failure to maintain Records	Persons deemed as intermediatary (such as an Internet Service Provider) must maintain required records for stipulated time. Failure is an offence.	Imprisonment up to three years, or/and with fine.
68	Failure/ refusal to comply with orders	The Controller may, by order, direct a Certifying Authority or any employee of such Authority to take such measures or cease carrying on such activities as specified in the order if those are necessary to ensure compliance with the provisions of this Act, rules or any regulations made thereunder. Any person who fails to comply with any such order shall be guilty of an offence.	Imprisonment up to three years, or/and with fine up to ₹ 2,00,000
69	Failure/ refusal to Decrypt Data	If the Controller is satisfied that it is necessary or expedient so to do in the interest of the sovereignty or integrity of India, the security of the State, friendly relations with foreign Stales or public order or for preventing incitement to the commission of any cognizable offence, for reasons to be recorded in writing, by order, direct any agency of the Government to intercept any information transmitted through any computer resource.The subscriber or any person in charge of the computer resource shall, when called upon by any agency which has been directed, must extend all facilities and technical assistance to decrypt the information. The subscriber or any person who fails to assist the agency referred is deemed to have committed a crime.	Imprisonment up to seven years and possible fine.
70	Securing access or attempting to secure access to a protected system	The appropriate Government may, by notification in the Official Gazette, declare that any computer, computer system or computer network to be a protected system. The appropriate Government may, by order in writing, Authorise the persons who are Authorised to access protected systems. If a person who secures access or attempts to secure access to a protected system, then he is committing an Offence.	Imprisonment up to ten years, or/and with fine.

Sec-tion	Offence	Description	Penalty
71	Misre-presentation	If anyone makes any misrepresentation to, or suppresses any material fact from, the Controller or the Certifying Authority for obtaining any license or Digital Signature Certificate.	Imprisonment up to three years, or/and with fine up to ₹ 1,00,000

Case Laws

Sandeep Varghese v State of Kerala in the High Court of Kerala the Petitioner was owner of a company and the respondent was an ex-employee of the company and had created a fake website with other accused and defamatory matter about the company was uploaded. Acts of forgery and impersonation was committed by the accused. Further fake email accounts of the Customer of the Company were created, through which emails were sent to malign the name of the Company. This caused immense damage to the name of the company. The company suffered crores of losses as the customers were unable to do business. Confidential information was also revealed by the respondent. They blackmailed the company and the directors. These are some of the types of issues that can crop up in any Business Organisation. In this context the author suggests the following Guidelines for Business Mangers.

Guidelines to Business Managers for Prevention of Cyber Crime

Cyber Security Group. Cyber Security Group should be formed as under [7] :-

(1) Publish particulars of Members.

(2) Incorporate at least one Member per Department or Task Group – preferably, the most knowledgeable.

(3) Responsibilities.

(a) Implementation of Physical Security and System Settings.

(b) A Cyber Security Auditor will be Nominated from each Department or Task Group. The Member of a Cyber Security Group belonging to a particular Department or Task Group will get all Information Technology Assets of his own Department or Task Group Audited from Auditor from

---

7. Sections 5, 10 and 11 of Information Technology Act 2000

another Department or Task Group in presence of the User of that Info Tech Asset as Nominated by him.

(c) Nominate Users for each Info Tech Asset based on utility of the Asset.

(d) Ensure Recording and Documentation.

(e) Specify Purpose of usage and ensure utilisation accordingly.

(f) Corrective Measures / Disciplinary Action on Cyber Security Lapses.

(g) Recruitment of Employees with Knowledge of Cyber Security.

(h) Individual and Collective Training and Refresher Programmes.

(j) Ensure Implementation of Password Policy to include Configuration of

Administrator Password – Administrator Credentials not to be Disclosed to the User.

(k) Audit of Computers by Team with at least one Member from another Department or Task Group before permitting Erasures, Formatting and Installation to prevent concealment or obliteration of evidence on Violation.

(l) Provision of Licensed Anti Virus to include Anti Malware, Anti Key Logger, Anti Root Kit, Anti Spyware for all Computers and facility to Update.

(m) Provision of Licensed Operating System and facility to Update.

(n) Surprise Checks.

(o) Ensure Delineation and Publication of Charter Duties for each Employee by every Departmental Head or Task Group Leader to determine utility of Info Tech Assets.

(p) <u>USB</u>. Disable Universal Serial Bus for all Storage Devices.

(q) <u>CCTV Cameras</u>. Installation, Maintenance and Monitoring of Close Circuit Television Cameras.

(r) Administrator Log In, Cyber Security Audit, Installations and Repairs only in presence of User.

(s) Frisking at Entry and Exit.

(t) <u>Investigations of Cyber Security Violations</u>. A Team will be constituted with overall Responsibility under a Team Leader by specifying the Nature of Violation and Purpose of Investigation.

(u) <u>SOP</u>. Formulate a Standard Operating Procedure on the Basis of the Act and obtain Undertaking of adherence to it from all Employees as part of Terms and Conditions imposed on the Employee, preferably at the time of Recruitment itself.

(v) <u>Channel of Reporting</u>. Establish a direct Channel of Communication for Reporting of Cyber Security Violations to Incident Reporters, Audit Teams and Investigation Teams.

(w) <u>User Access Control</u>. Ensure the following :-

(i) System Administrators are not Regular Users.

(ii) System Administrators are nominated for each Info Tech Asset.

(iii) Relief Programme of System Administrators for leave, Outstation Duties and Emergency Absence – Administrator Credentials to be known to the Main as well as Reserve Administrator, with Authority to Administer with the Main Administrator, unless he is Absent due to Emergency.

(iv) Maintenance of Relief Log of System Administrators.

(v) Regular Users do not get Administrator Rights and Credentials to include Passwords as well as User Names.

(vi) Names of System Administrators are Recorded in Device Log Books with Duration of Responsibility.

(vii) All System Administrators and Regular Users take an Undertaking withrespect to Administration Rights, Privileges and Credentials.

Recording and Documentation. [8]

(1) Procurement of Info Tech Assets based on detail Justification and Specification of Purpose.

(2) User Log Book. Following Information should be Recorded in a separate Log Book maintained for each Asset :-

(a) Particulars of the designated User to include Department or Task Group with duration of usage.

(b) Purpose of Utilisation.

(c) Device Information.

(i) Serial Number.

(ii) Model Number.

(iii) Manufacturing Company.

(iv) Date of Procurement.

(v) Memory Capacity.

(vi) Serial Number and Capacity of Hard Disk.

(vii) Physical Size and Dimensions.

(viii) Pixels and Diagonal Size of Video Monitor.

(ix) Type of Processor.

(x) Media Access Control id.

(xi) Capacity, Type, Frequency and Manufacturing Company of Random Access Memory.

(xii) Manufacturing Company of CD/DVD ROM/Writer.

(xiii) Version of Operating System.

(d) Date and Time of Installations and Repairs along with nature of Repairs carried out.

(3) Record of Cyber Security Audit with details of Devices Checked and Violations observed.

(4) Record of Disciplinary Action against Violations and Corrective Measures taken.

(5) Record of Print Outs with Details of the Document, Number Pages and Copies, Security

---

8. Section 16 of Information Technology Act 2000

Classification.

User Responsibility. [9]

(1) Cabinet Lock.

(2) Protection from loose Cabling, fire and dust – apprise Info Tech In Charge if conditions are beyond control.

(3) Visual Inspection every time before starting work.

(4) Classified Information is kept on a Compact Diskette under lock and key – not in the Computer.

(5) System Settings.

(6) Implementation of Password Policy. [10]

(a) At least 8 Characters.

(b) Mix of Capital and Small Letters.

(c) Mix of Digits, Letters of the Alphabet and Special Characters.

(d) Not related to Tasks, Departments, Names, Dates etc.

(e) Changed Periodically as determined by Cyber Security Group.

(f) Following Passwords will be Set Up :-

(i) Basic Input Output Setting.

(ii) System Key.

(iii) Windows User Log In for Standard User.

(g) All Default Passwords will be changed upon first use.

(7) Erasures, Formatting and Installations only on permission by Cyber Security Group.

(8) Self Checking and Cyber Security Group Audit before Handing and Taking Over of Computer.

(9) All Data is Encrypted using suitable Software.

(10) Updating of Operating System with Security Patches and Updating of Anti Virus.

(11) Record of Print Outs with Details of the Document, Number Pages and Copies, Security Classification.

(12) Maintenance of Log Books and Authentication of each Entry by Cyber Security Group.

(13) No Data pertaining to the Firm or its Employees to be carried outside the Premises unless Expressly permitted by Cyber Security Group.

(14) No Personal Information is stored.

(15) Never Login as Administrator except in presence of Cyber Security Group Member with at least one Member from another Department or Task Group and one from own exclusively for Installation, Formatting and Repairs.

(16) No Pirated Software will be used.

(17) No USB based Mass Storage Medium except for CD/ DVD ROM/ Writer will be used.

(18) All available Information will be given during Investigations of Cyber Security Violations.

Handling of Storage Media.

(1) Secondary Mass Storage Devices such as CD/DVD Writers, removable Ethernet based Hard Drives such as Network Access Storage (NAS) etc. to be kept under Lock and Key, preferably Sealed.

(2) Once out of Order or not in use, Storage Media will be disposed off securely in presence of the User and at least one Member of Cyber Security Group from the Department or Task Group as well as one Member from

---

9. Section 4 of Information Technology Act 2000

10. Section 6 of Information Technology Act 2000

another Department or Task Group when no longer required. The Storage Medium will be Damaged beyond Repairable Condition and Burnt.

(3) USB Based Storage except CD / DVD ROM/ Handy Cams, Card Readers, Secure Digital /Mini SD/ Micro SD Cards, Multi Media Cards, Personal Digital Assistants etc. Writers will be banned. This will include Cellular Mobile Phones, Digital Video

Investigations. [11]

(1) All Cyber Security Violations Reported and Identified by Auditors will invariably be Investigated under Instructions from the highest Authority – Incident Reporters and Cyber Security Auditors will have independent Chanel of Access to the highest Authority.

(2) Investigations to be carried out by Team to be Constituted by Cyber Security Group under a Team Leader – Employee involved with the Violation will not be an Investigator.

(3) Purpose of Investigation to be Specified for the Team.

(4) The Team will :-

(a) Investigate Circumstances under which the Violation took place.

(b) Determine reasons for Violations / Lapses.

(c) Fix Responsibility.

(d) Recommend Corrective Measures.

(5) Reports by the Team will be directly put up to the Highest Authority.

(6) Handling of Digital Evidence.

(a) All Digital Evidence will be seized by the Team.

(b) Digital Evidence will be properly Documented, photographed, Labeled – an Inventory will be prepared.

(c) It will be protected in storage and transportation from heat, humidity, Magnetic Fields, shocks or vibrations.

(7) Questionnaire will invariably be prepared to include clear Yes/ No type Questions with requirements of Explanation. Explanation will also be sought for abstention from Answering.

Miscellaneous Aspects.

(1) It is the responsibility of every Employee to Report any Cyber Security Violation Noticed by him directly to the highest Authority.

(2) No Information about the Firm Software to include Photographs of Premises or Work Place will be provided on Personal Domain and Social Networking Websites / Application. Exception at the Dicreation of Cyber Security Group can be Name, type of job and location.

(3) No Official Information including Photographs will be carried on person or shared by any Employee unless official duties warrant; provided it is specifically and expressly permitted by Cyber Security Group.

(4) All Info Tech Assets will be Locked and Sealed every time after Working Hours and the Seal will preferably be placed as well as opened

---

11. Sections 10 and 25 of Information Technology Act 2000

in presence of the User in addition to Cyber Security Group Member from the Department. If the User and Member is the same, then Member from another Department or Task Group can be present.

System Settings. [12] It is Recommended for Business Managers to set up all Computers based on **Microsoft Windows 7 Operating System** and above as per succeeding Paragraphs to avoid involvement of Employees in Cyber Crimes either Willfully or unknowingly. Licensed Software could be used or Info Tech Professionals could also be Contracted to carry out System Wide changes in Firms for Implementing Software Based Cyber Security Measures. However, Settings elucidated in the subsequent Paragraphs can be carried out by any Business Manager with basic knowledge of Computes without Professional Expertise in the Field. Following aspects should be kept in mind while carrying out the Settings :-

(1) To be effective and prevent malfunctioning of the Computer, the Settings must be done **in conjunction with each other in one go for each Computer** as most of theSettings are inter related.

(2) It will be necessary to Log On as **Administrator for Running the Command secpol.msc**.

(3) **Administrator Credentials will not be asked by the System in case the User is Loged On as an Administrator** for certain Settings.

Setting Up Passwords.

(1) BIOS Password. Enter BIOS Setup by repetitively pressing F 2 in quick succession as soon as the Central Processing Unit is turned on at System Startup – enter BIOS Set Up – enter Security – enter Passwords – select BIOS Password – Enter and confirm the Password

(2) SysKey. Run Command with Windows + R button or from Start Menu – type syskey – press OK – select Encryption Enabled Radio Button – press Update – select Password Startup Radio Button – Enter and Confirm

(3) Standard User and Administrator Passwords. Start Menu – Control Panel – Small Icons – User Accounts [- either of the following depending upon the Situation –]

(a) Change your Account Type (to Configure Administrator for such Privileges or Standard User to deny such Privileges to the Operative User)

(b) Manage another Account – Add User Account [or] –[select any of the existing Account]

Disable Guest Account. Choose and Disable in Manage another Account Menu of User Accounts from Control Panel.

Delete /Disable Users Accounts for Terminated Employees/ Employees not at Work. Right Click on My Computer Icon on Desktop –Manage – give Administrator Password – click OK – Local Users and Groups – Users – Right Click on the User – Properties [or - Select Delete] - Select Disable – click OK

Screen Saver. Start Menu – Control Panel –

---

12. www.quickheal.com – 31 Tips on Internet Security by Mr. Rajib Singha

Personalisation [or – Display – Personalisation] – Screen Saver – Select Blank from Drop Down List - Wait 1 Minute – Tick Mark the Check Box

On Resume Display Logon Screen – Click Apply – Click OK

Renaming Administrator. Start Menu – Control Panel –User Accounts – Manage another Account [or – click on the Operative Account] – click – Change Account Name – New Account Name – Change Name

Disable Auto Play. Start Menu – Control Panel - Small Icons - Auto Play – uncheck Use Auto Play for all Media and Devices Check Box –Drop Down all Lists one by one and Select Take no Action – click Save

Disable Remote Settings.Right Click on My Computer Icon on Desktop – Properties – Remote Settings –Remote Pane – click Allow Remote Assistance Check Box in Remote Assistance and Don't allow Remote Connections to this Computer Radio Button in Remote Desktop – click Apply – click OK

Selectively Disable USB Port. Windows + R [or – Start Menu – Run] –type regedit - click OK – HKEY_LOCAL MACHINE –SYSTEM – CurrentControlSet – Services – USBSTOR– Start – Select Hexadecimal Radio Button – Value 3 for Enabling Completely or 5 for Enabling only for Printers or 6 for Disabling all

Disable Audio / Voice Recording. Start Menu – Control Panel – Small Icons –Sound – Recording – click each Icon and set up one by one – Properties – General – Drop Down List – Don't use this Device (Disable) – Properties – Change Settings – give Administrator Password – click OK – Driver Pane - Disable

Set Up Interactive Log On. Run secpol.msc– Security Settings – Local Policies - Security Options – Interactive Log On

(1) Disabling User Information on Welcome Screen. Display User Information when ession Timed Out – Drop Down List – Select Do not by Clicking on it – Click on Apply – Click on OK

(2) Do Not Display Last User Name.Local Security Settings Pane – Enable Radio Button – Click on Apply – Click on OK

(3) Do Not Require Control + Alt + Delete.Local Security Settings Pane – Disable Radio Button – Click on Apply – Click on OK

(4) Machine Account Lockout Threshold. Local Security Settings Pane – 3 Invalid Lockout Attempts – Click on Apply – Click on OK

(5) Machine Account Lockout Limit.Local Security Settings Pane – 60 Seconds – Click on Apply – Click on OK

(6) Lockout Duration. Local Security Settings Pane – 10 Minutes – Click on Apply – Click on OK

(7) Prompt User to Change Password Before Expiration. Local Security Settings Pane – 15 days – Click on Apply – Click on OK

(8) **Disable the Following.**

(a) Require Domain Controller Authentication

(b) Require Smart Card

(9) **Smart Card Removal Behaviour.** None

Shut Down Settings. Run secpol.msc – Security Settings – Local Policies - Security Options – Shut Down

(1) Allow System to be Shut Down Without Having to Log On. Local Security Settings Pane – Disable Radio Button – Click on OK

(2) Clear Virtual Memory. Local Security Settings Pane – Enable Radio Button – Click on Apply – Click on OK

Password Policy Setting. Run secpol.msc – Security Settings – Account Policies – Password Policy

(1) Maximum Password Age. Local Security Settings Pane – 15 Days – Click on Apply – Click on OK

(2) Minimum Password Age. Local Security Settings Pane – 0 Days – Click on Apply – Click on OK

(3) Minimun Password Length. Local Security Settings Pane – 8 Charcters – Click on Apply – Click on OK

(4) Password Must Meet Complexity Requirements. Local Security Settings Pane – Enable Radio Button – Click on Apply – Click on OK

Account Lockout Policy Setting. Run secpol.msc – Security Settings – Account Policies – Account Lockout Policy

(1) Account Lockout Duration. Local Security Settings Pane – 10 Minutes – Click on Apply – Click on OK

(2) Account Lockout Threshold. Local Security Settings Pane – 3 Invalid Log In Attempts - Click on Apply – Click on OK

(3) Rese Account Lockout Counter. Local Security Settings Pane – After 10 Minutes – Click on Apply – Click on OK

(4) Password Must Meet Complexity Requirements. Local Security Settings Pane – Enable Radio Button – Click on Apply – Click on OK

Disable Certain Services. Right Click My Computer Icon – Manage – give Administrator Credentials – Services and Applications – Services – Disable the following Services :-

(1) Bluetooth Support
(2) Distributed Link Tracking Client
(3) Internet Protocol Helper
(4) SSDP Discovery
(5) Remote Auto Connection Manager
(6) Remote Desktop

Enable Firewall.Certain Versions of Anti Virus Software control Firewall. In such cases it will not be possible to Set Up Firewall Manually. However, it is desirable to be Enabled for all types of Network with Windows Default Settings.

User Account ControlSetting.Runsecpol.msc – Security Settings – Local Policies Security Options –User Account Control

(1) Administrator Approval Mode for Built in Administrator.Local Security Settings Pane – EnableRadio Button – Click on Apply – Click on OK

(2) Behaviour of the Elevation Prompt for Administrators in Administration Approval Mode. Local Security Settings Pane – Drop Down List – Prompt for Credentials on Secure Desktop - Click on Apply – Click on OK

(3) Behaviour of the Elevation Prompt for Standard Users. Local Security Settings Pane – Drop Down List – Prompt for Credentials on Secure Desktop - Click on Apply – Click on OK

(4) Detect Application Elevation and Prompt for Installations. Local Security Settings Pane – Enable Radio Button – Click on Apply – Click on OK

(5) Switch to Secure Desktop when Prompting for Elevation. Local Security Settings Pane – Enable Radio Button – Click on Apply – Click on OK

Web Browsers Setting.

(1) Must be Set Up to delete all Browsing History including Cookies, Auto Fill Forms Data, User Account Details, User Names, Passwords, Hosted Apps Data, User Assistance History etc from the beginning of Usage of the Computer and as soon as the Browser is closed. These Settings are usually available in the Settings, Options, Privacy, Tools or Security Menus of various Browsers.

(2) All Tracking, Usage Statistics and Performance Reports must be Disabled.

(3) All users must function in Incognito Window or In Private Browsing available in Safety, Privacy, Main or Options Menu.

(4) More than two Web Browsers should not be Installed.

Conclusion

As there is a large variety of Application Software and Web Browsers, this Article has not mentioned Settings peculiar to Apps and Browsers. However, by implementing these Guidelines and applying these Settings, shortcomings of such Peculiarities are by and large eliminated.

It is appreciated that these Guidelines and Settings will impose several Restrictions, Costs and Functional Inconvenience on Business Managers. However, the Advantages of Cyber Security undoubtedly outweigh the Disadvantages of Functioning under relatively Insecure conditions. It will be Prudent to choose the harder right by acting secure, despite inconvenience; instead of choosing the easier wrong and exposing the Organisation or its Members to legal action under Information Technology Act. Business Managers are strongly Recommended to make all necessary adjustments to incorporate these Guidelines and System Settings.

Security is more a matter of Sensitivity and a Continuous Process for Business Managers to remain Alert and on their toes always. They should Explore into taking as many more of Security Measures as possible. Guidelines and System Settings elucidated in this Article are by no means exhaustive and do not assure immunity from Cyber Crime. However, it creates a Platform for Business Managers to function in a secure environment. The Importance of making exhaustive and Objective Check Lists as well as SOPs towards that end, need not be over-emphasised

Bibliography

1. Water Information Sharing and Analysis Centre Publication, June 2002.

2. Article on Cyber Security Metrics and Measures dated 22 August 2008 by Paul E. Black, Karen Scarfone and MurugiahSouppayaofNational Institute of Standards and Technology, Gaithersburg, Maryland.

3. Article on 10 Cyber Security Measures That Every Small Business Must Take by Richard Davis dated 08 November 2014 @ ww.tech.co

4. Article on 4 Vital Cyber Security Measures Every Safety-Conscious Entrepreneur Needs to Take dated 19 September 2017 @ enterpreneur.com

5. Article on 7 Cyber-Security Measures That Could Save Your Startup From A Serious Setback dated by Mehul Rajput

6. Wikipedia the Online Encyclopedia @ *en.wikipedia.org*

7. Article on Cyber Security measures in Protection and Control IEDs by K. Hagman, L. Frisk, J. Menezes and M.M. Saha of ABB AB, Substation Automation Products, Sweden

8. Information Technology Act 2000, Amended 2008

9. Cyber Security, the only Solution to Safer and Effective Business, Published by IMED and Intelligence Quotient Systems Private Limited - Reference Text Book for Certificate Course in Cyber Security at Bharati Vidyapeeth's Institute of Management and Entrepreneurship Development

10. Dr. Rajlakshmi Wagh, 'TECHNOLOGICAL PROGRESS IN BRANDING – A CASE STUDY AND CYBER MANAGEMENT'.

11. International Journal of Advance Research, IJOAR.org ISSN 2320 – 91271 IJOAR © 2014 Volume 2, Issue 5 of May 2014, Online @ http://www.ijoar.org