ISSN NO: 2277 – 2510 VOLUME : 5 ISSUE: 2

DRIVE • FEBRUARY 2012

CONTENTS

ISSN NO: 2277 – 2510 VOLUME: 5 ISSUE: 2

DRIVE

Guest Editor's Note:

Mr. Hemal Patel,

CEO, Elitecore,

Ahmedabad

Lessons for an Entrepreneur:

An entrepreneur is one who organizes and manages an enterprise that involves risk, challenge, initiatives and obstacles. Moreover an entrepreneur is one who employs productive labour and is a creator of job opportunities. An entrepreneur has a new idea that creates something wonderful and beautiful. An entrepreneur has a greater value in any economy because of the innovation factor that is involved in the establishment of a business. An entrepreneur is an important ingredient in any country's development as there is increased competition which in turn results in increased productivity. Entrepreneurship is a good option for people because it channelizes their energy, creativity and fresh perspectives into innovations and problem solving which contribute to the growth and development of their country and the world at large.

Though entrepreneurs are innovative and creative, still are some important lessons that they need to learn without which they can never be successful. Entrepreneurs go through a grueling task right from the conception of the business idea to its implementation and later on managing the same to the fulfillment of their dreams and wishes. There is a lot of difference between a good business idea and a successful business. In between the two points there are many factors like challenges, flaws and gaps which must be overcome, rectified and filled. In spite of careful planning, close scrutiny, constant monitoring, persistent vigil and unwavering commitment, a business can fail. But entrepreneurs ought not to lose their faith because may be the idea has failed but the entrepreneurs are always successful. Moreover failures are great learning experiences and rather than being defensive about it, try to honestly discover the reasons for the loss. Perfection can never be attained and hence one has to learn from the loss, start again and look forward to the success of the next venture. One failed idea gives birth to many new ideas. The fact that many precious hours have been invested in the implementation of a new business idea should itself be a motivating force for entrepreneurs to go ahead even amidst failures.

It is wise to fail but foolish to repeat mistakes. In an entrepreneur's dictionary insanity is repeating the same mistakes and expecting different results. Once a mistake is made, it should be rectified and not repeated. Every mistake made is a progress towards enlightenment for like failures, mistakes teach great things. Mistakes push the entrepreneur towards his goal. The only true mistake that an entrepreneur can make is doing nothing for fear of failure. Suppress the negative thoughts and press towards your goals through positivity.

An entrepreneur is known by his distinct values like industry, perseverance, determination, courage, confidence and fortitude and these are the qualities that propel him to achieve great things. But a good entrepreneur should also know when to pause in his work and take time out of his frenetic schedule to spend quality time with his family, to pursue his other dreams and hobbies, to reconnect with himself and

others, and to rejuvenate his body, soul and mind. If not with passage of time his body and mind will not cooperate and it will then be a great blow to his business. There is no meaning in wearing oneself thin. A perfect balance should be maintained between his business and personal life. These will also help the entrepreneur to enjoy his work more and have a new perception thereby adding more purpose and meaning in what he does.

Successful entrepreneurs are always tuned to opportunities. They find great business opportunities even in causal remarks made while passing. They are resourceful enough to find ways for the resources needed for a good business idea. Once they find their ideas are taking them in a different direction, they lose no time in analyzing the opportunities available in that direction. In due course of time an entrepreneur should learn to accept and adopt change for change is a great source of viable opportunities.

One of the main characteristics of entrepreneurs is to stay focused. The focus should be on the final prize and the means to attain it. During the journey they will have to surmount obstacles, overcome hurdles, confront challenges, and find resources, and so can never lose focus which should be on the pinnacle of success. What happens most of the time is that entrepreneurs in their zeal to run their businesses successfully every day lose their focus on the end result. The most essential quality needed here is that entrepreneurs should be solution oriented. Every hindrance, obstacle, and problem should be seen as a challenge and an opportunity. They focus more on the ways to solve them and not on the solution that they lose themselves in the struggle for success. And sad to say some even buckle under pressure. Focus generates a lot of power that is needed for scaling new heights and treading unknown territory. Through their focus they help others stay focused on the target in spite of changes and setbacks whereby impenetrable barriers are penetrated. Such entrepreneurs are not distracted, bogged down and stressed and hence do not easily quit.

An entrepreneur is required to set high, clear, specific and challenging goals but which are realistic and attainable. Goal setting has unspeakable power for it decides the size, the success, the level, the growth, the expansion, the achievement, the significance, the impact and the expansion of your enterprise. The decision to use the appropriate strategy and tool to implement the business idea and to carry out the business depends on goal setting. Goal setting is the best tool to proactively deal with business challenges. Being proactive helps an entrepreneur to anticipate problems and setbacks which will also equip him to deal with them without suffering a great loss. Goals set should be appropriate to the current position of the business, the resources available and the skills possessed. The other aspect that goes hand in hand with goal setting is working towards those goals. An entrepreneur should push himself to realize those goals with steadfast commitment, perseverance and diligence.

To be a successful entrepreneur, an entrepreneur should possess certain characteristics. One of them is the ability to take risks. Any business idea comes with its own package of risks which is well realized by the entrepreneur. When he embarks on the journey of entrepreneurship, he knows quite well that is a journey beset with risks which is why the end prize becomes all the more sweet, worthy and rewarding. An entrepreneur takes more risks; the more is his profit and success. There is no success and profit without risks. But an entrepreneur should be careful in choosing the risks. He can choose risks that he can handle and manage and that are good for the further development and growth of the business. Business is not only about survival in the highly competitive world but also the remarkable changes and the impact it makes in the world for which risk is necessary. Risk which is the fundamental of any enterprise and hence without it an enterprise will fade into mediocrity.

Soon after the conception of a business idea, an entrepreneur should have the confidence to implement

and carry it forward. An entrepreneur should exude confidence which will boost the morale of his employees to work for him with more enthusiasm and to retain and gain new customers. Even in the middle of failure, an entrepreneur should have confidence in himself, his entrepreneurial skills and his business ideas. In the face of failure an entrepreneur should not lose hope but realize that the world of business teems with failures, disappointments, loss and setbacks. A self-confident entrepreneur does not wallow in failures, setbacks and loss but becomes more determined, resilient and focused and he comes out of his problems unscathed.

While carrying on with your business, there comes a point of time when you begin to realize that no matter what you do, your business will simply not pay off. When this happens no matter how much time and effort you had invested, you will have make a firm decision and abandon it. May be the entrepreneur had spent a many valuable hours conceptualizing the idea, implementing it and carrying it forward and he may have talked about his business to his family, friends, role models and mentors, but the inevitable and painful decision must be taken. The entrepreneur knows very well that his reputation is at stake and therefore it might look unavoidable to abandon the business or the business idea, but he will have to take the necessary to steps to terminate it to avoid greater loss and greater loss of face. Once the business begins to be wobbly an entrepreneur should not ignore the symptoms and should have the fortitude to halt it. The fact that many hours and efforts have gone into it is the reason why an entrepreneur should carry forward a sick business. Bringing a business to a premature end does not imply that the entrepreneur does not have the aptitude to be successful as a businessman.

An entrepreneur puts into his business all his time, resource and efforts to take it a great level. But this does not mean that he should neglect or ignore his own personal life, family, friends and dreams. If an entrepreneur fails to strike a balance between his personal life and business, no matter how successful and rich he is, it will not give him happiness and peace. Lack of happiness and peace can lead various other related symptoms like depression, mood swings, stress, frustration and dissatisfaction which are not healthy and if unchecked can prove to be destructive and fatal. In addition to the damage it does to one's personality, it also hinder the entrepreneur from realizing his full potential which when used can bring countless benefits. To have a healthy life, an entrepreneur should have perfect balance in all his dimensions.

There are certain things that an entrepreneur must do to have all his dreams and wishes fulfilled. The first thing he needs to do is understand the power of dreams. An entrepreneur should dream beyond his capabilities, current position, experience, background, resources and education even in midst of hitches and failures. He is the one who does not allow opposition, frustration and setbacks to deter him and cripple him. Dreams have the power to goad an entrepreneur stay focused and never lose confidence. Dreams give him the much needed encouragement, enhancement, stimulation and motivation to climb higher and higher the ladder of success till the pinnacle is reached. But the most vital aspect is that an entrepreneur should start acting on his dreams and should be careful not to fall into the trap of procrastination. Dreams let an entrepreneur realize what he wants, reinstates his belief in his self, to get the needed boost, to have a different perspectives on various facets of life and to measure his progress.

A mediocre entrepreneur is characterized by his thinking within the box. What makes an effective entrepreneur from other ordinary entrepreneurs is his ability to think out of the box. Thinking out of the box enables an entrepreneur to find the right situation, time, resources, workforce and support to implement his business idea even in adverse circumstances. It gives him the right perspective to channelize his energy, focus and efforts in the accurate direction, thus helping him take the right course of action. It empowers him to overcome challenges, obstacles and scarcities. Such entrepreneurs have the power to influence everyone

around and infuse the world with positive energy and ideas.

To make a difference between failure and success, an entrepreneur should be persistent in his endeavour to bring about the best. An entrepreneur is aware of the inevitable fact that his path is not smooth and easy. Before anything substantial is achieved, a lot is sacrificed and a lot is done on his part. He is not satisfied with his achievements and he likes to be ahead of his competitors and time. He looks at failure as a confederate who chisels him to gain the impeccable and flawless version of his self. Failure, disappointment, criticism and setbacks are part of his life that will give him perseverance in his quest for profit, fame, success and happiness. An entrepreneur may have qualities like confidence, faith, courage and aptitude to be successful, but without perseverance he cannot convert his dream to reality.

An entrepreneur should have unshakeable faith in his self, his enterprise and his people. This unshakeable faith will never let him down and as such he will never give up by learning to overcoming difficulties with grit. When other ordinary people or entrepreneurs buckle under the pressure of failure, a tough entrepreneur sees it an opportunity to expand his business. He bounces back from failures with more resilience, assurance, audacity and experience to take his business to greater heights. With astounding grace and poise a resilient entrepreneur treats failure and success, ebb and flow, praise and criticism, opportunities and challenges, highs and lows, obstacles and openings and profit and loss equally.

BY:

MR. HEMAL PATEL

CEO,

ELITECORE.

FROM THE CHIEF EDITOR'S DESK:

Pedagogy:

Pedagogy is the art or science of teaching. The term also refers to the strategies of instruction or the styles of instruction and the functions and works of a teacher and teaching. More importantly it means the appropriate use of the strategies of instruction. A teacher becomes more effective if the pedagogy chosen by him or her suits the students' learning ability, background knowledge, experience and goals. The main focus in on how to be a teacher and hence it becomes the cause of failure of the educational system. For what is needed is that the teacher has a very good understanding of the subject, knows how to monitor the progress and the level of understanding of students and help students who fall behind thereby minimizing the rate of failure and drop out. The fact that pedagogy is not given importance accounts for the reason for the failure of students to excel academically and drop out. It also tells why in spite of the technologically aided teaching learning process, students fail to shine.

Unfortunately pedagogy is misinterpreted. While pedagogy is about the strategies to impart knowledge, overemphasis has been on how to be a teacher. The effectiveness of a teacher is seen in the creation of an atmosphere that is conducive to learning, where the students feel liberated and that in turn paves the way for students' achievement and success, both academic and personal. Generally unvarying, well-ordered and planned lessons are seen as the best teaching aid to bring in results. But on the other hand, Teachers will have to customize their abilities and skills to suit the level, interests, basic knowledge and needs of the students to reap harvests.

To be effective teachers should spend time on choosing the best strategies and learn how to manage the course plan or the curriculum and at the same time reach the students individually and impart the lesson in accordance with the student's need and level. During the design of the curriculum, pedagogy should play a vital role and the teachers should be trained and prepared to impart lessons. Rather than depending on and investing in external teaching tools and technology, more focus should be on pedagogy to help students in better writing, expanded knowledge, increased

achievement, improved skills for the modern workplace, heightened motivation, enriched preparation for global citizenry, elevated problem solving and decision-making and augmented teaming and cooperation.

To make education more meaningful and relevant, the needs of each student should be figured out and strategies developed accordingly. Good and efficient teachers should be able to analyze and then choose the instructive strategy. There should be constant monitoring, analysis, supervision and intervention that will help each student have a cognitive development. Best returns are given when teachers create a class culture that is conducive, supportive, enlightening, liberating, encouraging and inspiring. It does not stop here because teachers will have to ensure that the learning is consistent, constant and continuous and this can be achieved by nurturing students. When this is done even the disadvantaged and average students will be able to excel. To make the instructive strategy more effective, teachers should match the strategy to the situation and instinct and empathy will help the teachers in choosing the right strategy which come after a deeper understanding of the aptitude and attitude of students.

It is not always that teachers teach amid bounty, facilities and state-of-the-art infrastructure. There are many teachers who have proved their worth and resourcefulness even amidst shortages and lack of facilities. It is what comes from within that makes a teacher effectual and not without. A teacher can create a world of difference with the shortages by turning them into challenges. It is the teacher's attitude towards teaching learning process, endeavour to deliver the best, explore the unknown, adapt the unknown to the present, herald in changes when needed and mould the students to accept them are what matter the most and make up for the shortages. With these a teacher can surmount any difficulties and challenges to pave the way for increased achievement. Along with these, a resourceful teacher always anticipates what might happen and hence is always armed with a backup plan.

A classroom abounds with energy that is dynamic and creative. A competent teacher orchestrates the different aspects of pedagogy to create an environment that is harmonious, resonant and vibrant to provide cutting edge to students and to have better all-round growth. But before a teacher can accomplish something vital has to be done on his or her part. A teacher to be more proficient should have a deep understanding of the subject matter and at the same time be more flexible to adapt the variety to students' ability and level of understanding. By doing so, a teacher can assist students to relate one idea to another and deal with misconceptions which in turn facilitate students to link ideas across fields and in everyday life. A teacher should have a comprehensive knowledge of the concepts, theories and principles of his or her own discipline and outside and then transform and transfer the knowledge to students in harmony with their goals, interests and needs.

To be an enhanced teacher, a teacher should assess, modernize, recreate and analyze his or her own teaching skills and go for renovation and innovation of the same. A teacher should also think about testing and evaluation as extensions of instruction and not as separate entities from the teaching learning process. This serves to identify the level of learning and understanding whereby a teacher also assesses his or her own performance simultaneously and the instructive strategies can be adjusted for different situations and needs.

Teaching is a challenging task while considering the fact that all the students are not the same. Differences may crop up because of different backgrounds, families, culture, creed, intelligent quotient and attitude towards learning. Amidst these myriad of differences a teacher should being them all together and help them learn for which a teacher should have a sound knowledge of different learning processes and materials. Different learning materials for different purposes can be used to achieve the goal, but the most important point to be noted is the choice of appropriate learning material for different contexts. A talented teacher has knowledge about curriculum resources and technologies and fashions an interface between the students and the sources of information and knowledge. By doing so the teacher assist the students to explore new ideas, acquire new knowledge and fuse information to make them compatible for learning and make them relevant for day-to-day living. Delivering the content according to the strengths and weaknesses of different learners, a teacher helps students arrive at conclusion, solve problems and make decisions.

The foremost discussion that disturbs everyone and for which there is no permanent answer is whether pedagogy is benefitted by technology. Technology can only serve as a tool to deliver the message and it can never take the place of pedagogy, for it is the resourcefulness, innovative approach and creativity of the teacher that makes pedagogy more consequential, purposeful and applicable. But sad to say, technology often controls pedagogy rather than pedagogy controlling the way technology is used. The potential of technology can never be realized to the full, for it has its own limitations and restrictions. The need of the hour is a pedagogy that is technology free for technology cannot be relied upon because of its very nature. But also to be remembered is, if a teacher comes across a technology that will enable him or her to teach better and serve the purpose, it can be implemented. But that technology has to provide new and stimulating resources for learning, engage students better, give more scope for problem-solving and decision-making, explore new terrains, give access to better source of learning and knowledge and give a comprehensive view of the subject matter, it is to be encouraged. Care should be taken to ensure that technology is not promoted more than pedagogy for nothing can usurp the personal touch that human beings alone can provide. Learning becomes all the more fun and viable with a human touch. Flexibility of pedagogy makes in possible to strike a personal cord in students and reach out to them.

BY:

DR.NIKHIL ZAVERI

DIRECTOR & PRINCIPAL,

SEMCOM.

SEMCOM Updates:

Debate Competition:

Debate Competition was conducted on 11th January 2011and the coordinators were Ms. Nishrin Pathan, Ms. T. Hepzibah Mary and Mr. Dipan Bhatt. There were ten teams for the final competition and the Judges were Prof. Sudhir Mukherjee and Ms. Arti Vyas. In team participation, Pooja T. Nandi and Sebin Binny (FYBCom A) bagged the first prize and the second and third prizes were bagged by Vrunda R. Bhatt and Priyanka P. Tailor (TYBBA – General) and Bhagyashree Kadam and Shail N. Patel (SYBBA – General) respectively. In individual performance, the first three positions were given to Aashvi P. Thakrar, Pooja T. Nandi and Priyanka P. Tailor respectively. Principal's Special Prize was given to Pooja T. Amin and Drashti Sherdiwala (SYBBA – General) for team performance and Yash V. Chavda (SYBBA – ITM) for individual performance.

Global Gujarat Management Conclave:

Global Gujarat Management Conclave was organized from 24th January 2012 to 27th January 2012 and was coordinated by Mr. Sarvesh Trivedi. The main theme of the Management Conclave was Business Without Boundaries, Opportunities@Business.com. Under the Management Conclave many events were conducted which saw the enthusiastic participation of many students and key note addresses given by many eminent experts from various fields. The E-Biz Summit was on 24th January 2012 for which the Honourable Chairman, Dr. C. L. Patel, Charutar Vidya Mandal, was the President and Mr. Kiruba Shankar, CEO, Kiruba.com, Chennai was the key note speaker. It had two sessions and in the first session there were two experts namely, Mr. Rohan Bhansali, Co-Founder, GoZoop.com, Mumbai, who spoke on "Social Network for Business Footwork" and Mr. Manish Desai, AIRCEL, Ahmedabad, who spoke on "Mobile Technology for Business Growth". The second session saw two experts namely, Mr. Dipak Rai, Vice President-IT (Rtrd.), RIL, and Mr. Dhanya Thakkar, President, Indusface, Vadodara. They spoke on "Emerging Technology Platforms for Existing Business Stations" and Information "Security at the Business Front" respectively.

On 25th January 2012 there were two major events, Faculty Symposium and Novellus, The Ad Making Show. Faculty Symposium had two parts, Research Paper Contest and Teaching Innovation Contest and Prof. I. C. Gupta, Indore, was the key note speaker who was also one of the judges and the other judge was Dr. Darshana Dave. The coordinators for Faculty Symposium were Ms. Palak Patel and Mr. Sunil Chaudhary. Mr. Jay Vasavada was the key note speaker for Novellus, The Ad Making Show, Eminent Journalist and Speaker and he delivered his address on "The World of Advertisement". Dr. Vigna Oza, Dr. Swati Parab, Ms. Komal Mistry and Ms. Priyanka Nair were the coordinators.

Two events were conducted simultaneously on 26th January 2012, Technofest and Best Corporate Training Award Contest. All the IT faculty members of SEMCOM were the coordinators of Technofest under which many competitions were organized. Dr. Kamini Shah, Ms. Nishrin Pathan and Dr. Ajayraj Vyas were the coordinators.

The much awaited Elecon Best Business Idea was conducted on 27th January 2012 for which the Honourable Chairman, Dr. C. L. Patel, Charutar Vidya Mandal, was the President, Mr. Phanikumar, CEO, MHE Division, Elecon Engineering Co. Ltd. the Chief Guest and Mr. Hemal Patel, CEO, Elitecore Technologies Pvt. Ltd., Ahmedabad, the key note speaker. Dr. Kamini Shah, Dr. Shubash Joshi, Mr. Nilay Vaidya, Mr. Renil Thomas and Mr. Yogesh Patel were the coordinators. 11 business ideas were present out of which three best business ideas were selected and each team received a cash award of Rs. 25,000/- sponsored by Elecon.

On the evening of 27th January 2012 prize was distributed to the winners of various events that were conducted during the four days of Global Gujarat Management Conclave.

Green Business Fair:

SEMCOM always believes in pioneering and innovation in education that will help in cognitive development of the students and enable them to have exposure to the latest theories, inventions, discoveries that are prevalent in the world. It has added another feather to its cap by organizing a very innovative event called the Green Business Exhibition, the first of its kind. The objective behind this novel idea was to spread the awareness of green business initiatives taken by the Government and companies. It began with a grand note on 2nd February 2012, with its inaugural ceremony which was attended with great enthusiasm and expectation. It was organized in GCET College Auditorium, Vallabh Vidhyanagar. It indeed proved to be a great learning experience. Dr. Nikhil Zaveri, Principal and Director, SEMCOM, welcomed the guests and introduced them to the audience.

The key note speaker was Mr. Sushil Kumar, President (Operations), Reliance Industries, Dahej Plant. In his key note address the talked about the importance of environment and the immediate need to save the environment from destruction which is the offshoot of development. His main focus was on sustainable development. The Honourable Chairman, Dr. C. L. Patel, Charutar Vidya Mandal, was the President of the event. In his Presidential address he stressed that it is the young generation today who has the potential, the power and the determination to take good care of the environment since they are more exposed to the dangers posed by pollution. Dr. Suvashri Das, one of the coordinators, talked in length about the event - how it was organized. It was followed by Vote of Thanks proposed by Ms. Hiral Patel, a coordinator of the event. The event culminated with the national anthem.

The Green Business Exhibition cum Sale was on 2nd and3rd February 2012. The exhibition showcased green products which drove home the point the need to use green products that will not harm the environment and that will contribute to sustainable development. 35 groups of students represented companies like Suzlon, GNFC, GFL, Elecon, ITC Ltd., Kribhco, etc. and showcased the green products and the green services of these companies. During the exhibition the green products, green services and green initiatives of different companies were highlighted which will enable people to appreciate our environment more and also contribute towards saving our Mother Earth, which is the need of the hour.

Smart Eye Photography Contest:

In order to enhance creativity in the field of photography, Dr. Nikhil Zaveri, Director and Principal, SEMCOM, initiated a novel competition called Smart Eye Photography Contest this year. The competition was launched on 12th July 2011 which was followed by enormous response with 56 teams being registered. The theme for the contest was "Environment". 20 teams were selected for the final competition. The contest was inaugurated under the banner of Green Business Exhibition on 2nd February 2012. The exhibition was open on 2nd and 3rd February 2012. The photographs were judged by Mr. Sunil Adesara, a freelance photographer, Mr. Kanu Patel, a well-known artist and Mr. Priyesh Balakrishnan, Founder Director of Open Circle Communications, Ahmedabad. The contest was coordinated by Dr. Vigna Oza, Dr.S waty R. Parab, Ms. Komal Mistry and Ms. Priyanka Nair.

Mid Semester Examination:

The Mid Semester Theory Examination for the II and IV Semester students were conducted from 6th February 2012 to 9th February 2012 and the coordinators were Dr. Yashasvi Rajpara and Mr. Yogesh Patel. The Practical Examination for IT subjects and Communication Skills were conducted on 10th and 11th February 2010. The coordinators were the subject teachers concerned.

15th Annual Day:

It was a matter of immense pride and happiness that SEMCOM celebrated its 15th Annual Day on 13th February 2012, Monday. Since its inception in 1997, SEMCOM had always striven to impart quality education and along with it ample opportunities for cognitive development of students. It is the deep rooted faith of SEMCOM that to be consistent in imparting quality education innovation is very vital. True to its mission and vision SEMCOM had organized many events and undertaken many activities throughout the academic year. 13th February 2012 was the day when the success of these was relished and enjoyed. CA Mahesh P. Sarda, Partner, Delloitte Haskins & Sells, Chartered Accountants, Mumbai, was Chief Guest and Honourable Chairman, Dr. C. L. Patel, Charutar Vidya Mandal, was the President of the grand occasion. The splendid ceremony was spearheaded by Dr. Nikhil Zaveri, Director and Principal, SEMCOM. Dr. Yashasvi Rajpara, President, Students' Council, and the Students' Council coordinated the event.

Book Review:

FIVE POINT SOMEONE – WHAT NOT TO DO AT IIT!

About the Author:

Chetan Bhagat is the author of following blockbuster novels:

- Five Point Someone – what not to do at IIT! (2004),
- One Night @ the Call Center (2005)
- The 3 Mistakes of life (2008)
- 2 States – the story of my marriage.

Chetan also writes various columns for leading English and Hindi newspapers, focusing on youth and national development based issues. Many of the issues raised by Chetan's columns have been discussed in Parliament and among the top leadership of the country. New York Times called him the "biggest – selling English – language novelist in India's history".

Publication Details:

"Five Point someone" – What not to do at IIT!

- First in Rupa Paperback 2004
- 149th Impression 2009
- Published by Rupa Co., New Delhi, 110002
- Price (India): Hardcover Rs 295, Paperback Rs 95
- Pages: 270
- Written by Chetan Bhagat

'Five Point Someone' is a story about three friends in IIT who are unable to cope. In other words it describes how bad things can get if you don't think straight.

This Book has inspired one of best Bollywood film – '3 Idiots'.

About the Cover: The three gears represent Hari, Alok and Ryan, while the flower represents Neha. Also, gears need to mesh together to work, representing Hari, Alok and Ryan's friendship.

The white color of the cover represents simplicity, as seen in the writing style of the book. The definition of friendship spread all over reinforces the theme of the book.

About the Book:

The book starts with a disclaimer, "This is not a book to teach you how to get into IIT or even how to live in college. In fact, it describes how screwed up things can get if you don't think straight."

The book has three protagonists – Alok, Hari and Ryan, and is presented as a narrative of their experiences at IIT by Hari. The story describes the ups and downs of their college life which include their low scores and the way they are perceived by students and professors on the account of their scores, their tactics to beat the academic system including trying to steal their HoDs cabin and many such anecdotal as well as serious experiences.

About the Protagonists:

The novel has been written from point of view of narrator called Hari Kumar. Hari is fat, not very bright intellectually and a confused guy who makes it to IIT. He is fascinated by his friend Ryan who is carefree, confident, and smart with athlete structure. All he wants to do is be like Ryan and can never say "no" to him.

Ryan Oberoi is rich, brilliant, creative with full of new ideas who loves engineering. But he hates the education system as he feels it does not encourage original ideas and offers no scope for innovation. Moreover the system also judges students on the basis of their ability to mug up theoretical aspects and the grades they get.

Alok Gupta is poor, has paralytic dad and an elder sister of marriageable age. His mother is the sole bread earner in the household and always looks for Alok's

help. Alok wants to be an artist but decides to join the IIT because he feels that it is the only way he can get a good job and support his family.

Neha happens to be the daughter of Prof. Cherian, the domineering head of the Mechanical Engineering Department. Despite this, Hari attempts to woo Neha and eventually they fall in love.

The Story:

IIT's use a unique method of evaluating students called Grade Point Average or GPA. The score one gets is based on the performance of the entire class (it is not an absolute score). The top performer would get somewhere in high 9 point something and the bottom performers would be in 5 point something. Such people are disdainfully referred to as 5pointers and thus the title of the book, Five Point Someone.

The novel is set in the Indian Institute of Technology, Delhi during the period of 1991 to 1995. It is about the adventures of three mechanical engineering students and friends, Hari (the narrator), Ryan and Alok. Ryan is smart and outspoken, whereas Alok and Hari are crybabies and are willing to follow Ryan.

The book is narrated by Hari, with some small passages by his friends Ryan and Alok, as well as a letter by Hari's girlfriend Neha Cherian. The story revolves around their lives on campus starting from their elation on making it to one of the best engineering colleges in India which is quickly deflated by the rigor and monotony of academic work.

Most of the book deals with the numerous attempts by the trio to cope with and/or beat the system as well as Hari's fling with Neha who just happens to be the daughter of Prof. Cherian, the domineering head of the Mechanical Engineering Department.

While the tone of the novel is humorous, it takes some dark turns every now and then, especially when it comes to the families of the protagonists. Most of the action, however, takes place inside the campus as the boys, led by the ever creative Ryan, frequently lamenting how the internationally lauded IIT system has stifled their creativity by forcing them to value grades more than anything else. Uninspiring teaching and numerous assignments add to their woes, though the boys do find a sympathizer in Prof. Veera, the new professor of fluid mechanics

Summary and Conclusion:

'Five Point Someone' is a tale of three friends who come together at IIT. It unfolds in the action-packed four year period from their entry to graduation. There are certain aspects of the book and the author's writing which I feel are good.

First, the language is authentic and very simple. The narration of Hari is often presented in dialogue which conveys a sense of continuity and oneness. Also, his portrayal of typical college life (and not just IITs) is universal with commonly used lingo like 'insti', disco' etc.

The author has also added a blend of college romance, academic struggle and the confusion of what to do next in a very entertaining manner, spiced up with a task-master teacher and a smart mentor. The title of course is based on grading systems in IITs, where five pointers are among the laggards in a class. The grade becomes almost a caste system that one has to live with for the rest of one's life!

It is a novel which would make you laugh and for those who have stayed in hostel, this novel would make you take ride back to your memory lane. The most important thing of this novel is that it addresses serious issues like the Indian academic system and its pressures, peer pressure, ragging, etc. But it is represented very skillfully and with a funny touch.

What I liked about the book is that it does not try to justify or give excuses for the wrong doings of the protagonist. They are far less than perfect people, yet you come to like them and therein lies the greatness of the author.

The convocation speech at the end effectively summarizes the message of this book – 'to believe in self regardless of the social parameters of success', the importance of family, friends, personal goals and ambitions', 'not judging people quickly as well as based on their material success' and lastly, 'to not to take oneself very seriously'

BY:

MR. CHETAN PATEL,

LECTURER,

SEMCOM

Article:

Six Sigma

Introduction

Management has always evolved in itself by leaps and bounds only after a fall. History of the world has close relationship for the development of the field termed management which in itself is an outcome of the history. Management and management thinkers have devised various theories in areas related like production, finance, marketing human resource and many more. 'Six Sigma' evolved as a controlling technique which later on took the shape of enhancing quality and cost reduction technique.

'Six Sigma' originated as a set of practices designed to improve manufacturing processes and eliminate defects, but its application was subsequently extended to other types of business processes as well. In Six Sigma, a defect is defined as any process output that does not meet customer specifications, or that could lead to creating an output that does not meet customer specifications.

History

The idea of Six Sigma was actually "born" at Motorola in the 1970s, when senior executive Art Sundry was criticizing Motorola's bad quality. Through this criticism, the company discovered the connection between increasing quality and decreasing costs in the production process. Before, everybody thought that quality would cost extra money. In fact, it was reducing costs, as costs for repair or control sank. Then, Bill Smith first formulated the particulars of the methodology at Motorola in 1986. Six Sigma was heavily inspired by six preceding decades of quality improvement methodologies such as quality control, TQM, and Zero Defects, based on the work of pioneers such as Shewhart, Deming, Juran, Ishikawa, Taguchi and others.

The term Six Sigma originated from terminology associated with manufacturing, specifically terms associated with statistical modeling of manufacturing processes. The maturity of a manufacturing process can be described by a sigma rating indicating its yield, or the percentage of defect-free products it creates. A six sigma process is one in which 99.99966% of the products manufactured are statistically expected to be free of defects (3.4 defects per million). Motorola set a goal of "six sigma" for all of its manufacturing operations, and this goal became a byword for the management and engineering practices used to achieve it.

Doctrines

Six Sigma doctrines assert that:

Continuous efforts to achieve stable and predictable process results (i.e., reduce process variation) are of vital importance to business success.

Manufacturing and business processes have characteristics that can be measured, analyzed, improved and controlled.

Achieving sustained quality improvement requires commitment from the entire organization, particularly from top-level management.

Methods

Six Sigma projects follow two project methodologies inspired by Deming's Plan-Do-Check-Act Cycle. These methodologies, composed of five phases each, bear the acronyms DMAIC and DMADV.

DMAIC is used for projects aimed at improving an existing business process. DMAIC is pronounced as "duh-may-ick". DMADV is used for projects aimed at creating new product or process designs. DMADV is pronounced as "duh-mad-vee".

DMAIC: The DMAIC project methodology has five phases:

Define the problem, the voice of the customer, and the project goals, specifically.

Measure key aspects of the current process and collect relevant data.

Analyze the data to investigate and verify cause-and-effect relationships. Determine what the relationships are, and attempt to ensure that all factors have been considered. Seek out root cause of the defect under investigation.

Improve or optimize the current process based upon data analysis using techniques such as design of experiments, poka yoke or mistake proofing, and standard work to create a new, future state process. Set up pilot runs to establish process capability.

Control the future state process to ensure that any deviations from target are corrected before they result in defects. Implement control systems such as statistical process control, production boards, and visual workplaces, and continuously monitor the process.

DMADV or DFSS: The DMADV project methodology, also known as DFSS ("Design For Six Sigma"), features five phases:

Define design goals that are consistent with customer demands and the enterprise strategy.

Measure and identify CTQs (characteristics that are Critical To Quality), product capabilities, production process capability, and risks.

Analyze to develop and design alternatives, create a high-level design and evaluate design capability to select the best design.

Design details, optimize the design, and plan for design verification. This phase may require simulations.

Verify the design, set up pilot runs, implement the production process and hand it over to the process owner(s).

Role of the 1.5 sigma shift: Experience has shown that processes usually do not perform as well in the long term as they do in the short term. As a result, the number of sigmas that will fit between the processes mean and the nearest specification limit may well drop over time, compared to an initial short-term study. To account for this real-life increase in process variation over time, an empirically-based 1.5 sigma shift is introduced into the calculation. According to this idea, a process that fits 6 sigma between the process mean and the nearest specification limit in a short-term study will in the long term only fit 4.5 sigma – either because the process mean will move over time, or because the long-term standard deviation of the process will be greater than that observed in the short term, or both. Hence the widely accepted definition of a six sigma process is a process that produces 3.4 defective parts per million opportunities (DPMO). This is based on the fact that a process that is normally distributed will have 3.4 parts per million beyond a point that is 4.5 standard deviations above or below the mean (one-sided capability study). So the 3.4 DPMO of a six sigma process in fact corresponds to 4.5 sigma, namely 6 sigma minus the 1.5-sigma shift was introduced to account for long-term variation. This allows for the fact that special causes may result in deterioration in process performance over time, and is designed to prevent underestimation of the defect levels likely to be encountered in real-life operation.

Sigma levels: A control chart depicting a process that experienced a sigma drift in the process mean toward the upper specification limit starting at midnight. Control charts are used to maintain 6 sigma qualities by signaling when quality professionals should investigate a process to find and eliminate special-cause variation.

The table below gives long-term DPMO values corresponding to various short-term sigma levels.

It must be understood that these figures assume that the process mean will shift by 1.5 sigma toward the side with a critical specification limit. In other words, they assume that after the initial study determining the short-term sigma level, the long-term Cpk value will turn out to be 0.5 less than the short-term Cpk value. So, for example, the DPMO figure given for 1 sigma assumes that the long-term process mean will be 0.5 sigma beyond the specification limit (Cpk = –0.17), rather than 1 sigma within it, as it was in the short-term study (Cpk = 0.33). Note that the defect percentages only indicate defects exceeding the specification limit to which the process mean is nearest. Defects beyond the far specification limit are not included in the percentages.

Sigma level	DPMO	Percent defective	Percentage yield	Short-term C_{pk}	Long-term C_{pk}
1	691,462	69%	31%	0.33	–0.17
2	308,538	31%	69%	0.67	0.17
3	66,807	6.7%	93.3%	1.00	0.5
4	6,210	0.62%	99.38%	1.33	0.83
5	233	0.023%	99.977%	1.67	1.17
6	**3.4**	**0.00034%**	**99.99966%**	**2.00**	**1.5**
7	0.019	0.0000019%	99.9999981%	2.33	1.83

BY:

MR. RENIL THOMAS

LECTURER,SEMCOM

Article:

Computer Hacking Threat to Security System

INTRODUCTION:

Computer Hacking:

Computer hacking is defined as any act of accessing a computer or computer network without the owner's permission. [1]

Computer hacking is the practice of modifying computer hardware and software to accomplish a goal outside of the creator's original purpose. People who engage in computer hacking activities are often called hackers. Since the word "hack" has long been used to describe someone who is incompetent at his/her profession, some hackers claim this term is offensive and fails to give appropriate recognition to their skills.

Since a large number of hackers are self-taught prodigies, some corporations actually employ computer hackers as part of their technical support staff. These individuals use their skills to find flaws in the company's security system so that they can be repaired quickly. In many cases, this type of computer hacking helps prevent identity theft and other serious computer-related crimes. [2]

A brief History

One might not suspect that the art, or scourge, of computer hacking was created at one of the havens for technological excellence.

True, at MIT (Massachusetts Institute of Technology), a group of students developed the technique and borrowed their name from the "hackers" of the late 1800s who found amusement in pranking the emerging telephone companies. Getting their laughs and skills from hacking and cracking into primitive computers and exploiting the Arpanet (predecessor to the internet), they created a novelty that would become the target of federal crackdown in years to come. However, the act of hacking started out innocently, and was basically a method of trying to figure out how computer systems worked. The 1970s saw the rise in "phreaking," or phone hacking, headed by John Draper. This method allowed the user of a "blue box,", when used with a Captain Crunch whistle of 2600 hertz which accessed the AT&T long distance system, to make free long distance calls. Hackers initiated with accessing the free phone calls through a varied range of sources, thereby managing to circumvent into the nation's radio system and the phoning system resulting in a tremendous phone fraud nationwide.

After the age of "phreaking," computers became not only the target, but also the forum, for a growing hacker population to communicate. The creation of bulletin board systems (BBS) allowed this communication and the technological possibility of more serious government and credit card hacking became possible. At this time in the early 80's, hacking groups such as the Legion of Doom began to emerge in the United States, giving organization, and thus more power to hackers across the country.

Once this happened, breaking into the computers became a legitimate activity, with its own groups and soon its own voice with the 2600 magazine, launched in 1984. The effects of computer hacking were serious. Two years later, inevitably, Congress launched the Computer Fraud and Abuse Act that outlawed hacking. Over the years, there was a series of noticeable occurrences as the worst consequential effect of computer hacking on more high profile cases, such as the Morris Worm, responsible for infecting government and university systems, and the Mitnick case in 1995, which captured Kevin Mitnick, steeling as many as 20000 credit card numbers.

In 1999, security software became widely known by the public, and with the release of new Windows programs, which were littered with security weaknesses, they became successful because of necessity. This fraudulent act of computer hacking is perhaps the major problem, confronting the rapidly expanding population of Internet users today, with the systems still trying to battle online hackers. [3]

Computer Hackers

Forensic science utilizes the global resources of the Internet to access databases and to communicate with concerned experts. This form of communication, however, can make forensic databases and files vulnerable to deliberate sabotage. Computer hackers are people who gain remote access (typically unauthorized and unapproved) to files stored in another computer, or even to the operating system of the computer. In the 1950 and 1960s, hackers were motivated more by a desire to learn the operating characteristics of a computer than by any malicious intent. Indeed, in those days hackers were often legitimate computer programmers who were seeking ways of routing information more quickly through the then-cumbersome operating systems of computers.

Since then, however, computer hacking has become much more sophisticated, organized, and, in many cases, illegal. Some hackers are motivated by a desire to cripple sensitive sites, make mischief, and to acquire restricted information.

In the late 1990s, several computer hackers attempted to gain access to files in the computer network at the Pentagon. The incidents, which were dubbed Solar Sunrise, were regarded as a dress rehearsal for a later and more malicious cyber-attack, and stimulated a revamping of the military's computer defenses. In another example, computer hackers were able to gain access to patient files at the Indiana University School of Medicine in February 2003.

One well-known hacker is Kevin Mitnick. Beginning in the late 1970s and continuing through the late 1980s, Mitnick was apprehended at least five times for hacking into various computer sites. Indeed, his lenient one-year jail sentence and subsequent counseling was based on his defense that he suffered from a computer addiction. In 1989, he vanished, only to reappear in 1992, when police became suspicious of tampering with a California Department of Motor Vehicles database. Mitnick was arrested in 1995 and remained in prison until his release in 2002. He was barred by law from using a computer until January 21, 2003 and later published. The Art of Intrusion: The Real Stories behind the Exploits of Hackers, Intruders, and Deceivers in 2005.

The U.S. Patriot Act was signed into law on October 26, 2001. The intent of the act was to curb the danger posed to the country by terrorism. Computer hackers did not escape the legislative crack-down, since hacking represents a potential national security threat.

Under the act's provisions, the power of federal officials in criminal investigations involving hacking activities has been increased. These increased and somewhat secretive powers were among the contentious issues debated in 2005 as provisions of the Patriot Act come up for renewal.

Indeed, the threats to civilian privacy and national security from computer hackers was deemed so urgent that the U.S. government further enacted the Cyber-Security Enhancement Act in July 2002, as part of the Homeland Security measures in the wake of the terrorist attacks on September 11, 2001. Under this legislation, hackers can be regarded as terrorists, and can be imprisoned for up to 20 years. In seeking to prosecute a suspected hacker, investigators have the power to conduct Internet searches or telephone taps without court-sanctioned permission.

One tool that a hacker can use to compromise an individual computer or a computer network is a virus. Depending on their design and intent, the

consequences of a virus can range from the inconvenient (i.e., defacing of a web site) to the catastrophic (i.e., disabling of a computer network). Within a few years during the 1990s, the number of known computer viruses increased to over 30,000. That number is now upwards of 100,000, with new viruses appearing virtually daily.

Despite the threat that they can pose, computer hackers can also be of benefit. By exposing the flaws in a computer network, hackers can aid in the redesign of the system to make information more inaccessible to unauthorized access. [3]

Types of Computer Hacking

Hacking threats can come from inside or outside an organization, but malicious hacking, of any kind, is a felony in the United States and many other countries.

1. Ethical Hacking

Ethical hacking refers to the penetration, or attempted penetration, of an organization's computer systems by an authorized individual with the full knowledge and consent of the organization concerned. Ethical hacking is often authorized so that an organization can better understand its own security vulnerabilities and the damage that can be done to its systems if a hacker is able to break in.

2. Denial of Service

A denial of service attack occurs when one or more computers bombard a Web server with so many requests that the server cannot process legitimate requests and the service it provides is denied to legitimate users.

3. IP Spoofing

IP spoofing is the practice of impersonating, or spoofing, the Internet Protocol (IP) of a computer so that any Internet traffic sent from that computer appears to have come from somewhere else. Hackers may spoof an IP address to cause a computer to believe that it is effectively talking to itself, causing its operating system to freeze or crash. IP spoofing can also be used to hijack an Internet session by attacking a computer once it has been authenticated and stealing its identity.

4. Identity & Intellectual Property Theft

Another form of hacking involves breaking into a computer system expressly to steal sensitive, personally identifiable information, such as credit card numbers, or intellectual property- such as patents, trademarks and other copyrighted material. This information can be used, or sold for fraudulent purposes, such as financial, medical or character identity theft, or for industrial espionage. Hacking of this type may also include phishing, which involves sending unsolicited email messages to victims, inviting them to visit a certain website. The website appears legitimate, but is specifically designed to gather information without the knowledge or consent of the victim or download malware. The effects of phishing may remain hidden from victims until they discover that their bank or credit card accounts have been emptied. [4]

Types of Computer Hackers

The term hacker is a generic term to describe attackers. Not all have intent to steal your data. Below is a list of various types of hackers.

1. White Hat

White hat has the skills to break into computer systems and do damage. However, they use their skills to help organizations. For example a white hat might work for an organization to test for security weaknesses and vulnerabilities in the network.

2. Black Hat

Black Hat also known as a cracker uses his skills to break into computer systems for unethical reasons. For example, steal user data like, username and password, credit card numbers, bank information.

3. Grey Hat

This type can be thought of as a white hat attacker who sometimes acts unethically. They could be employed as a legit network security administrator. But, during this person's duties, he may find an opportunity for gaining access to company data and stealing that data.

4. Phreaker

A phreaker is simply a hacker of telecommunications. An example of this is tricking the phone system into letting you make free long distance calls.

5. Script Kiddy

A Script Kiddy is someone who lacks the skills of a typical hacker. They rely on downloading hacking programs or utilities sometimes calls scripts to perform an attack.

6. Hacktivist

This is a person with political motivations, such as someone defacing a website and leaving messages on the hacked site for the world to see.

7. Computer Security Hacker

This is someone who knows the technical aspects of computer networking and security. This person could attack a network protected by a firewall or IPS by fragmenting packets.

8. Academic Hacker

This type is typically an employee or student at an institution of higher education. They would use the institutions computing resources to write malicious programs.

9. Hobby Hacker

This is someone that tends to focus more on home computing. Such as, modifying existing hardware or software, use software without a license, unlock Apple iPhone. [5]

Computer security

Computer security is a branch of computer technology known as information security as applied to computers and networks. The objective of computer security includes protection of information and property from theft, corruption, or natural disaster, while allowing the information and property to remain accessible and productive to its intended users. The term computer system security means the collective processes and mechanisms by which sensitive and valuable information and services are protected from publication, tampering or collapse by unauthorized activities or untrustworthy individuals and unplanned events respectively. The strategies and methodologies of computer security often differ from most other computer technologies because of its somewhat elusive objective of preventing unwanted computer behavior instead of enabling wanted computer behavior. [6]

Network Security

Security is an important ingredient for computer network (LAN, WAN, MAN) maintenance. It is the job of the network administrator to save your online presence from malicious attacks of hackers, viruses, and Trojans through a reliable security system. Network security is the study of implementing different techniques to save your business and home computers from malicious hacking and virus's attacks. Here is a brief overview of some common network attacks.

1. Denial of services

2. BlackHat Hacking

Network hackers with technical knowledge can easily access any unsecured network. Common network damage involves configuration change in network equipment like router servers. They usually make these devices unavailable for internet users. Some hackers even get access to private information like patient/client record, or credit card details. These damages can cost thousands of dollars to your company. At home, these network hackers try to steal your sensitive information like credit cards and other scanned documents.

3. Firewall

It is called a set of principles to deny or allow access to the network. It is usually installed inside the network router. The basic purpose of using a router is to get access to the network. Whenever any internet user stops using a network protocol for communication, the router closes the port of this protocol.

4. Access Control Lists

Access control list works like a firewall. Its basic function is to filter network traffic based on various metrics included in IP packets. Access control list is configured to test the secure status of each packet (data segmentation on OSI layers) and IP address

destination. It also checks the destination and source port number. Usually a network administrator writes an access control list and specifies the range of IP addresses communicating to each other and the protocols used in this communication session. In such situations, it becomes quite tough for network hackers to get access to a network in which the router is blocking unauthorized access.

5. Encryption

It is an easy and simple algorithm used to convert information into an unreadable format. Only a person who has access to the specific algorithm can decrypt it. Always try to send sensitive information through these encryption techniques.

6. WEP / WPA

These days, wireless networks are widely used due to their portability features. It is also necessary to protect your wireless network from hackers. Recent research indicates that a new version of wireless network called WPA2 is more secure than its previous version (WEP). When you are setting your wireless network, you must set your security to WPA2. [7]

Computer Security System

One of the most popular computer uses is associated with security video equipment. Wireless video cameras will transfer the video stream directly to computers. With the right software of digital computers will be able to record properly all the video information sent there or just activate the recording only when the software detects every move (recording begins only when there is a change of the video image). [8]

Types of Security Systems

In today's technical world, there are a variety of security systems on the market. There are systems for the home, the car and even personal systems that can be worn on the body. Following are the types of systems available.

Motion sensors detect movement in the home or on the property. Some of these systems use infrared light that detects changes in heat. High frequency wave is another motion sensor.

1. Wireless Security Systems

These systems are convenient because they can be put almost anywhere and can be moved when necessary. There are no wires to worry about hiding, or getting tangled with other wires in the home.

2. Acoustic Sensors

These sensors can detect sounds such as breaking glass. These sensors are us doors where intruders are likely to try and gain entrance into a home or business.

3. Digital Security Systems

These systems secure a certain area and require a code to disarm them. If this is not done, the company that monitors the device, will check for an error or send help, if necessary.

4. Personal Alarms

These alarms are carried around with a person and in the event that there is a medical or other emergency, the alarm can be triggered. These are usually worn on the body, either the neck or wrist. [9]

Sources of Information (Survey)

In this research paper, we have used secondary source (online survey references) to examine the Computer Hacking Threat to Security System.

1. Hacking Hits 90% of US Businesses

- According to a June 2011 survey released by Ponemon Research on behalf of Juniper Networks, 90 percent of companies surveyed said they had been hacked in the past 12 months. In addition, 59 percent said they had been hit by multiple hacking attempts. {via PCWorld}

- The researchers surveyed 583 IT professionals and IT security practitioners. More than half (51 percent) were employed by companies with over 5,000 employees.

- With such an onslaught of hacking activity, companies have been forced to compensate by hiring more full-time security IT staff, by planning with cash outlays in case of attack, and by investing in high-tech security

software–all of which increase overhead. According to the same study, 41 percent of respondents said these hacking prevention measures cost more than $500,000, and an additional 16 percent said they could not calculate the costs.

More than one third (34 percent) of the respondents said they have low confidence in their IT infrastructure's ability to prevent a network security breach. IT professionals say their organizations are left vulnerable because of a lack of resources and because of the complexity of implementing security measures. [10]

2. 2011 Set to Be Worst Year Ever for Security Breaches

The worst three cyber security incidents of the year so far have involved RSA, Epsilon and Sony.

In mid-March, Boston-based cryptography firm RSA suffered a massive network intrusion that resulted in the theft of information related to its SecurID tokens. Forty million people use the tokens to access the internal computer networks of 25,000 corporations, government organizations and financial institutions.

Two months later, defense contractor Lockheed Martin had its own networks penetrated by attackers who used "cloned" RSA tokens made with data taken in the original breach.

In early April, hackers penetrated the internal networks of Epsilon, a Texas-based firm that handles email communications for more than 2,500 clients worldwide. The companies affected by the Epsilon hack included Ameriprise Financial, BestBuy, Capital One Bank, Citi, JPMorgan Chase, TiVo, U.S. Bank and dozens more.

Last (but not least in the eyes of some gamers) is Sony. Since early April, the Japanese entertainment and electronics giant has been fighting different groups of hackers. One group stole the personal information of 102 million registered users of the Play Station Network (PSN) and other online gaming services.

Other organizations that have had their security compromised in 2011 include NASA's Goddard Space Flight Center, which lost confidential satellite data in an April hack, and InfraGard, an FBI affiliate that was compromised by the hacking group LulzSec, which also attacked PBS, Nintendo and Fox.

3. Cybercrime Blotter: High-Profile Hacks of 2011

June 9: Britain's National Health Service

LulzSec put on the "white hat" for this intrusion. It alerted the NHS that its network security was inadequate and publicized the hack without revealing any compromising information. The group's @lulzsec Twitter feed also solicited bone-marrow donors in honor of a 15-year-old English girl dying of cancer whose "bucket list" blog had drawn attention.

June 9: Citigroup

The banking and insurance giant announced that unknown hackers had penetrated its network security and made off with the personal identification information of some 200,000 clients.

June 8: Canada's Conservative Party

Hackers apparently upset by Prime Minister Stephen Harper's moves to regulate the Internet in Canada -- and by his re-election -- broke into his party's servers, planting a bogus story about how he had to be rushed to the hospital after choking on hash browns at breakfast.

June 6: Nintendo

Nintendo became LulzSec's second major target of the first week of June. On June 6, LulzSec compromised the U.S. servers of the gaming giant Nintendo. No

information was stolen, and LulzSec admitted on its Twitter page that it "didn't mean any harm."

June 3: InfraGard

LulzSec strikes again! On June 3, the hacktivist group defaced the website of InfraGard, an Atlanta-based firm that provides IT security to the FBI. In addition to defacing the site, LulzSec leaked 700 megabytes of emails from InfraGard, as well as the personal information of 180 employees.

June 1: L-3 Communications

Just days after hackers penetrated the networks of Lockheed Martin, U.S. defense contractor L-3 Communications admitted that it had suffered a network intrusion.

June 1: Google Gmail

Chinese identity thieves used "spear phishing" to take over hundreds of Gmail accounts, including those belonging to senior American officials, Chinese political activists, military personnel and journalists.

May 29: PBS

LulzSec didn't waste any time after hitting Fox in early May; on May 29, the hacking group defaced the PBS website with a phony news story claiming that slain rapper Tupac Shakur is alive and living in New Zealand.

May 27: Lockheed Martin

Lockheed Martin, the largest provider of IT services to the U.S. government and military, suffered a network intrusion stemming from data stolen pertaining to RSA's SecurID authentication tokens.

May 17: NASA

A Romanian hacker calling himself "TinKode" took to Twitter on May 17, boasting that he had breached a computer server at NASA's Goddard Space Flight Center and gained access to confidential satellite data used to aid in disaster relief.

May 17: Massachusetts Executive Office of Labor and Workforce Development

Hackers used a Trojan to get into the network of the state labor agency, exposing the names, addresses, email addresses and Social Security numbers of an estimated 210,000 people.

May 16: Her Majesty's Treasury

Britain's Chancellor of the Exchequer, George Osborne, announces that the British treasury ministry has been under sustained cyber-attack for months. He tells a conference that the ministry was receiving about 20,000 "spear phishing" emails per month, rigged with malware to open backdoors into the organization's networks, but that none had gotten through.

May 13: Fox Broadcasting Company

LulzSec breaks into a server hosting Fox.com and publish about 400 email addresses and passwords belong to employees of the Fox Broadcasting Company and local affiliate stations.

May 9: Anonymous

A disgruntled follower of the hacktivist movement turned on the group and took over message boards where Anonymous members chatted and planned attacks.

May 5: Sony

In what Sony called a third attack on its servers, an Excel spreadsheet showing the names and hometowns of entrants in a 2001 Sony-sponsored prize contest was posted online.

May 4: "The X Factor"

The hacking group LulzSec burst onto the scene on May 4 by stealing the names, emails and phone numbers of a quarter-of-a-million contestants of Fox's Simon Cowell-hosted singing competition "The X Factor." A week later, LulzSec would admit to hacking

Fox Broadcasting Network and stealing the usernames and passwords of nearly 400 Fox employees.

May 2: Sony Online Entertainment

Sony suddenly disconnects the network linking players of massive multiplayer games. It turns out the network's back end was breached at the same time as those of the PlayStation Network and Qriocity networks were, bringing the total number compromised accounts to 102 million.

April 25: New York Yankees

Major League Baseball's most successful (and sometimes most-hated) team struck out on user privacy when a team employee accidentally emailed an Excel spreadsheet containing the contact information for more than 21,000 season-ticket holders. The attachment went to about 2,000 business contacts, but the Yankees were quick to state that no birth dates, Social Security numbers or financial information were among the data.

April 20: PlayStation Network and Qriocity

As a result of possibly the largest data breach ever, Sony suddenly took its PlayStation Network and Qriocity on-demand entertainment services offline on April 20. Two days later, Sony explained that there had been an "external intrusion" that had forced the shutdown of the networks. On April 26, it announced that intruders had accessed the user records of up to 77 million users, whose real names, email addresses, passwords, home addresses and telephone numbers had all been stored in unencrypted text. Sony said the associated credit-card numbers had been encrypted, even as hackers offered purported Sony-associated credit-card numbers in online bazaars and anecdotes came in of mounting credit-card fraud among PlayStation Network users.

April 17: Oak Ridge National Laboratory

One of the main servers at the Department of Energy-run research facility near Knoxville, Tenn., was taken offline after administrators noticed large amounts of data in the process of being stolen. The lab was originally built to process plutonium for nuclear weapons, but now focuses on civilian nuclear, biological, chemical and information-technology research.

April 17: European Space Agency

A Romanian "gray hat" hacker - one who takes things mainly to embarrass their owners - got into the servers of the European Space Agency outside Paris, then posted user names, account information and passwords on his own website after letting ESA administrators know.

April 13: WordPress.com

WordPress.com, which makes and distributes the popular WordPress blogging platform, announced on April 13 that hackers had broken into the servers of Automattic, which host WordPress-based blogs. The intruders potentially made off with sensitive information such as source code and user passwords of WordPress' 25 million bloggers. This is the second major attack on WordPress.com in the past two months. In March 2011, WordPress.com was hit by a massive distributed denial-of-service attack.

April 4: Sony

Anonymous-affiliated hacktivists use DDoS attacks take down several PlayStation-related websites in retaliation for Sony's lawsuit against hacker George Hotz, who discovered the internal password to "jailbreak" the PlayStation 3 and posted the password online.

March 30: Epsilon

At least 26 companies, including BestBuy, Capitol One Bank, Citi, JPMorgan Chase, TiVo and Walgreens, have their customer email lists stolen during a data breach

at Epsilon, which handles e-mail communications for 2,500 companies worldwide. Passwords or other sensitive data was not taken, but security experts warned of an upsurge in spam and phishing attacks in the coming months.

March 29: Australian Parliament

Sydney's Daily Telegraph learns that sophisticated hackers, thought to be working for Chinese intelligence, had for nearly two months been intercepting messages sent over the federal parliamentary email system. Ten members of Parliament, including Prime Minister Julia Gillard and Australia's foreign and defense ministers, had their parliamentary computers compromised.

March 27: MySQL.com

MySQL.com, the main website promoting the open-source database-management software suite, is hacked into by two Romanian "gray hat" hackers using, ironically, a SQL injection. SQL injections are common but powerful Web-based attacks that exploit overlooked "holes" in a website's database communications. The hacked caused no damage but did embarrass Oracle Corp., which owns and distributes MySQL.

March 25: RIAA.com

Anonymous-affiliated hacktivists use a DDoS attack to bring down the website of the Recording Industry Association of America for about five hours. Anonymous said the attack was to protest a new RIAA lawsuit against the shuttered file-sharing service LimeWire, which demanded damages of $150,000 for each download of some 11,000 copyrighted songs -- a claim estimated at $75 trillion dollars.

March 24: New Zealand Department of Internal Affairs

Anonymous-affiliated hacktivists had promised to punish New Zealand's civil-service department for a new law that mandated Internet censorship of possible child pornography.

March 24: TripAdvisor.com

The popular travel-planning website revealed that network intruders had made off with part of the membership email list. No passwords or financial data were compromised, according to the company, but it did warn members to be ready for an uptick in spam.

March 23: European Commission, European External Action Service

On the eve of a major summit of European leaders to discuss the escalating crisis in Libya, the executive and diplomatic bodies of the European Union in Brussels came under sophisticated attack.

March 17: RSA

RSA, maker of SecurID authentication tokens, said its networks had been penetrated, and data stolen, by an "advanced persistent threat" (i.e., hackers likely sponsored by the Chinese government). The company would not say if the breach affected the 40 million SecurID tokens used by employees of large corporations and government agencies to log into secure networks and systems, or the 250 million smartphones that use a similar system.

March 17: Hollywood Starlets

Up to 50 young female celebrities had nude photos stolen from their email and smartphone accounts. "High School Musical" star Vanessa Hudgens was said to be talking to the FBI.

March 7: French Finance Ministry

Sophisticated hackers used "spear phishing" attacks to penetrate and steal sensitive documents from the French finance ministry.

March 4: South Korea

Directed denial-of-service (DDoS) attacks hit various websites in South Korea, including the presidential residence the Blue House and the country's two largest search engines.

March 3: WordPress

The popular blogging service got taken down for several hours by what company founder Matt Mullenweg called the "largest and most sustained" DDoS attack in its six-year history.

February 24: Westboro Baptist Church

On Feb. 24, Anonymous took down several websites associated with the controversial Westboro Baptist Church.

February 22: Voice of America

On Feb. 22, pro-Iran hackers went after 'Voice of America' the official news service of the United States government.

February 18: Canada

In mid-February, it was revealed that the Treasury Board, Finance Department and Defence Research and Development — Defence Research and Development Canada is a civilian military agency. The hackers were seeking confidential information pertaining to financial and weapons information and data about oil and gas resources.

February 11: Iran

As antigovernment protests spread throughout the Middle East, so did cyber-attacks aimed at crippling oppressive government regimes. The distributed denial-of-service (DDoS) attacks were levied against the websites of IRNA.

February 6: HBGary Federal

On Feb. 5, Aaron Barr, chief executive of the Washington, D.C.-based security firm HB Gary Federal, announced that he had unmasked the members of Anonymous, and would reveal their identities at a security conference later in the month. Wasting no time, Anonymous the following day took down the website of Barr's company, hijacked Barr's personal Twitter account and his boss's LinkedIn profile, and posted more than 70,000 of Barr's personal e-mails. In a brazen show of defiance, Anonymous even posted the dossier of secret Anonymous identities Barr was planning to make public.

February 5: Nasdaq

Next up to go down: the Nasdaq. As reported in a Feb. 5 Wall Street Journal article, hackers for the past year had been targeting computer networks belonging to the Nasdaq stock exchange. But these online crooks weren't after money. The hackers' real target was Directors Desk, a cloud application owned by Nasdaq that stores financial records and reports for hundreds of Fortune 500 companies and more than 10,000 corporate board members.

January 26: Utah, Michigan, Albania, Italy, the U.S. Army, etc.

A few weeks passed before another high-profile organization was targeted, but when the next hit came, it was a big one. In late January, a hacker hijacked more than a dozen top military, government and education websites. The hacked websites were being sold for $55-$499 each on an underground market.

January 26: Egypt

On Jan. 26, Anonymous struck again, this time against Egypt's official government websites. The attacks on the websites of the cabinet, Ministry of the Interior and Ministry of Communications and Information Technology were carried out after then-President Hosni Mubarak blocked citizens' access to Twitter.

January 2: Tunisia

The first notable digital disruption of the year occurred just two days in, when the hacktivist group Anonymous launched massive DDoS attacks against at least eight Tunisian government websites. [11]

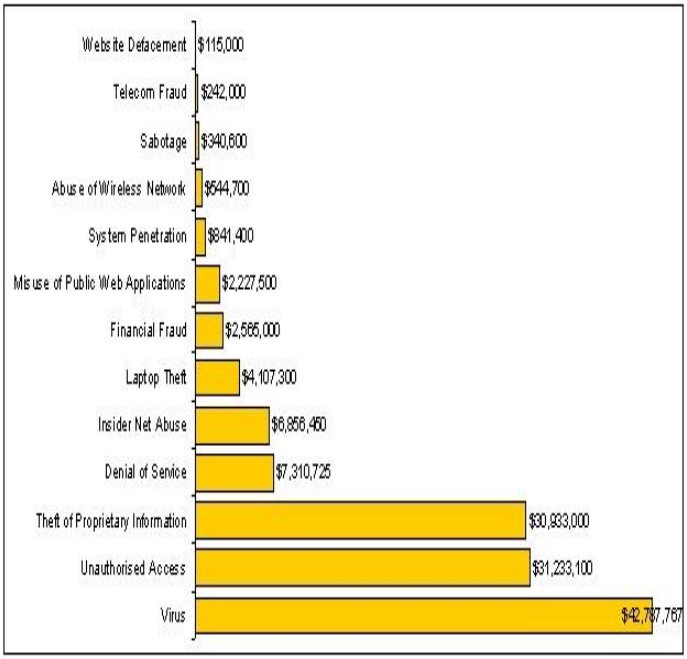
4. Quarter of UK kids have tried hacking, survey finds

Twenty-six percent of children surveyed said they had tried hacking -- breaking into someone else's account -- at some point. Of those who had hacked, more than a quarter (27 percent) had targeted accounts on the popular social networking site Facebook, and 18 percent went after their friends' e-mail accounts, the survey found. The most common reason for hacking was for fun, with 46 percent of respondents giving that answer. But 21 percent said they intended to cause disruption and 20 percent thought they could generate an income from hacking, the survey found. [12]

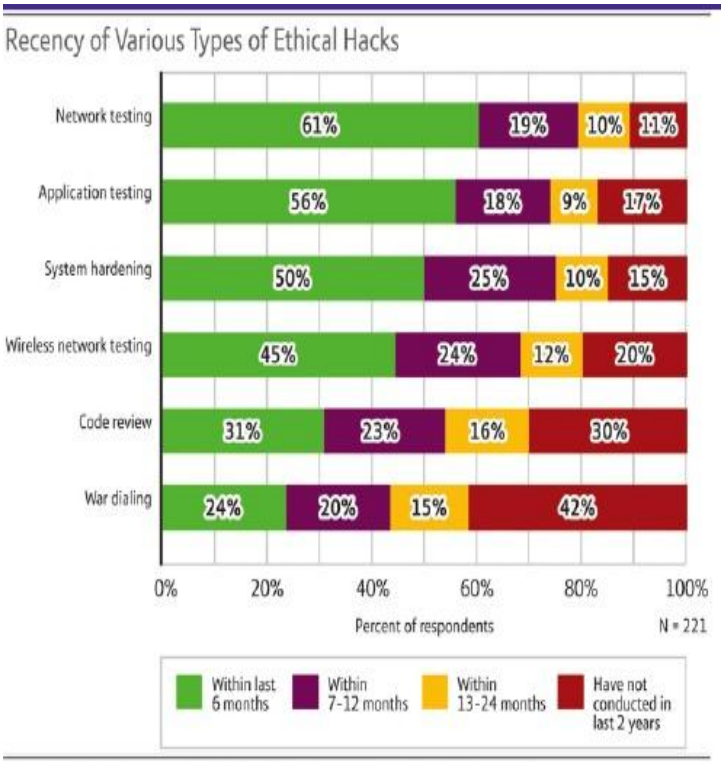
5. Insider Threat to Computer Security

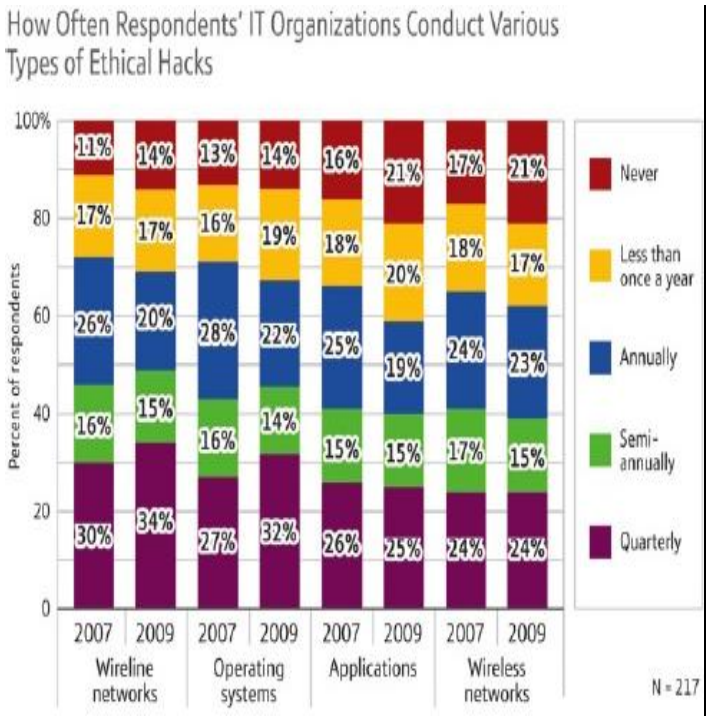
The Computer Security Institute and FBI cooperate to conduct an annual CSI/FBI Computer Crime and Security Survey of U.S. corporations, government agencies, financial institutions, and universities. 80% cited disgruntled and dishonest employees as the most likely source of attack on their computer system. Fifty-five percent of respondents reported unauthorized access by insiders, as compared with 30% reporting system penetration by outsiders. Many companies reported multiple instances of unauthorized access or system penetration. [13]

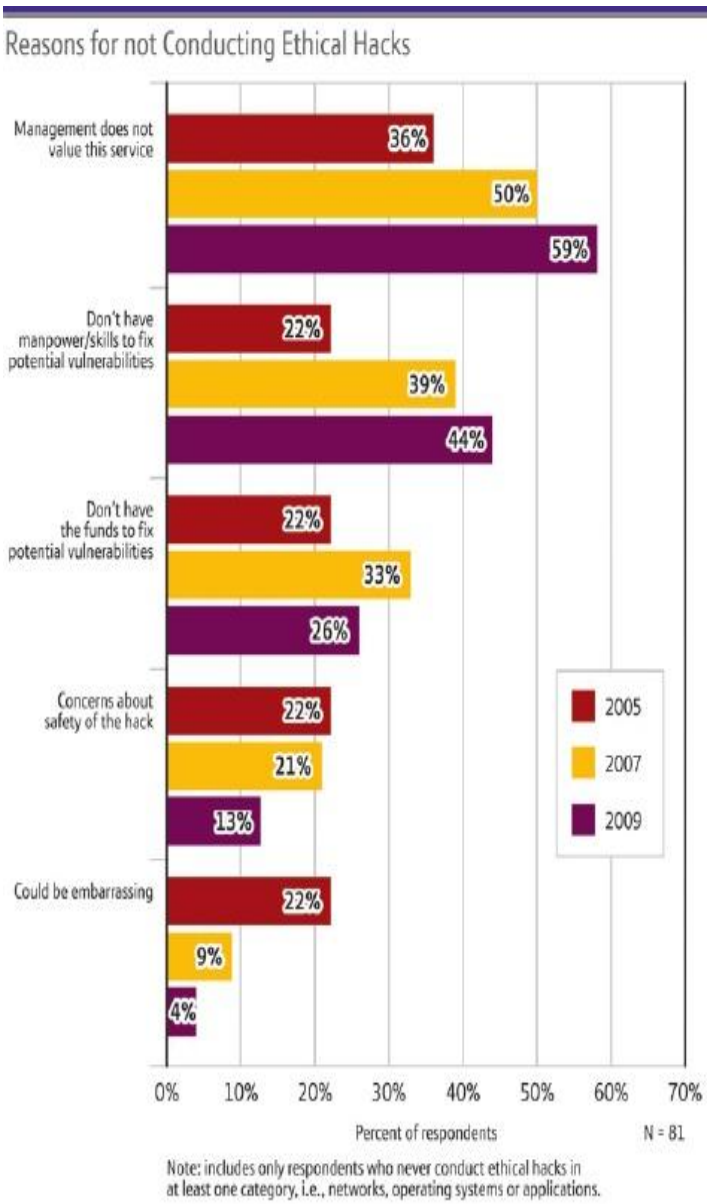
6. The figure shows the total losses as reported by the 2005 CSI/FBI Annual Computer Crime and Security Survey. [14]

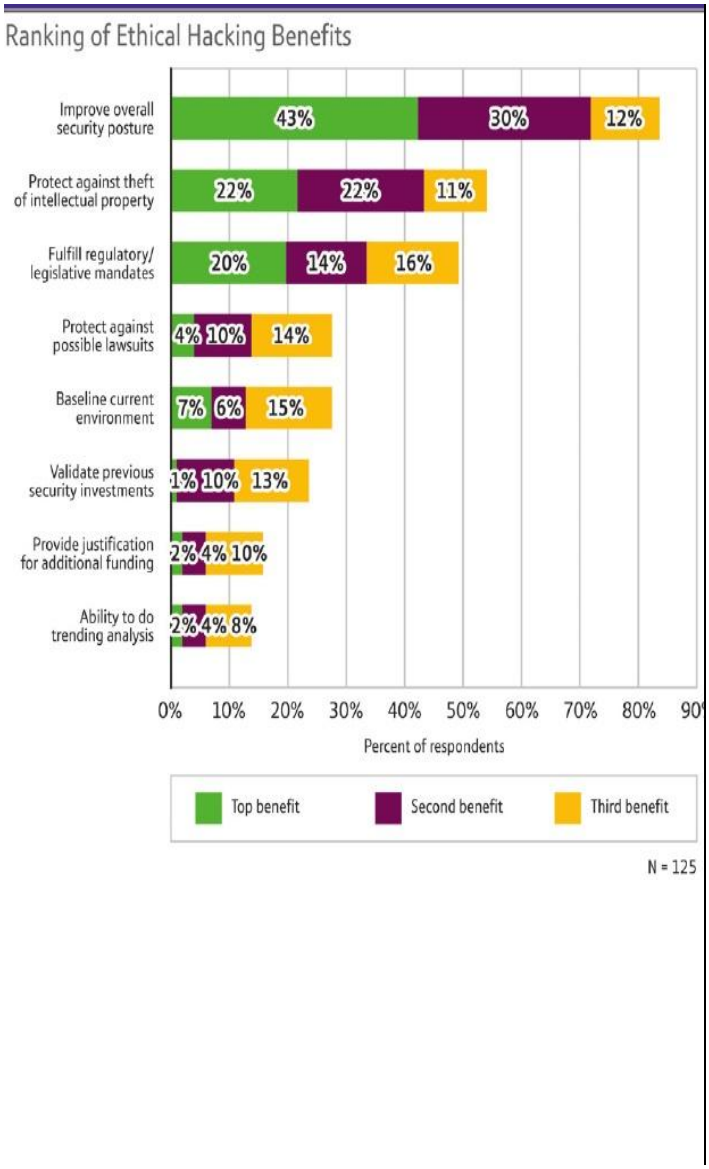


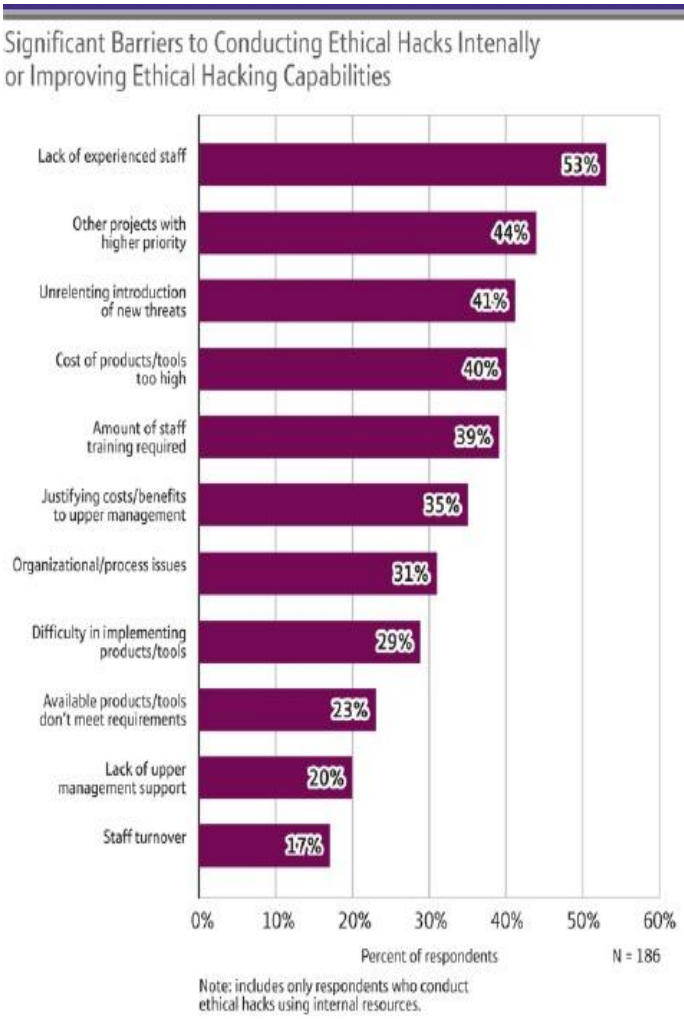
7. Ethical Hacking [15]

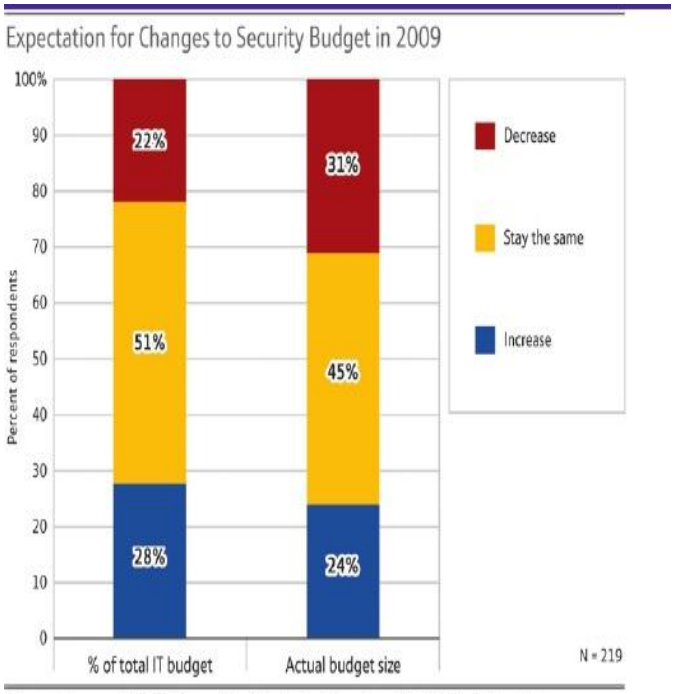


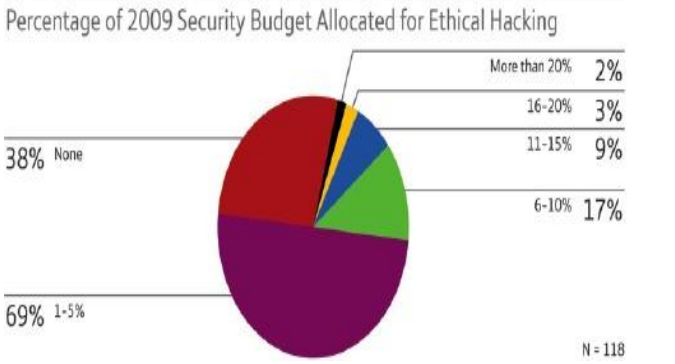

How Often Respondents' IT Organizations Conduct Various Types of Ethical Hacks
Percent of respondents
100%
80
60
40
20
0
11%
14%
13%
14%
16%
21%
17%
21%
17%
17%
16%
19%
18%
20%
18%
17%
26%
20%
28%
22%
25%
19%
24%
23%
16%
15%
16%
14%
15%
15%
17%
15%
30%
34%
27%
32%
26%
25%
24%
24%
2007
2009
2007
2009
2007
2009
2007
2009
Wireline networks
Operating systems
Applications
Wireless networks
Never
Less than once a year
Annually
Semi-annually
Quarterly
N = 217

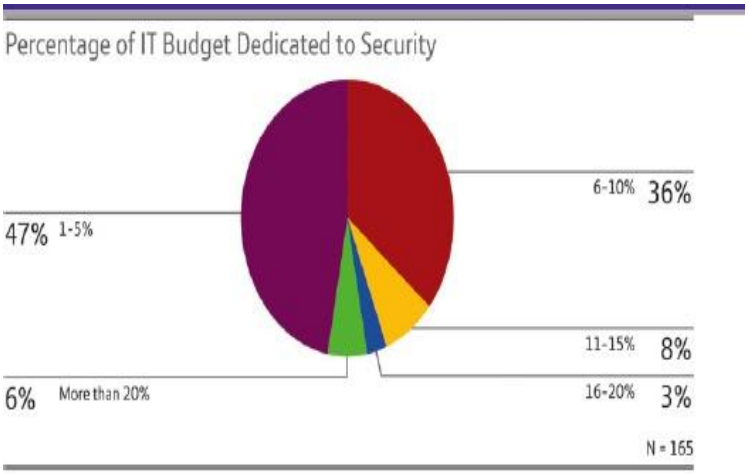

Reasons for not Conducting Ethical Hacks
Management does not value this service
36%
50%
59%
Don't have manpower/skills to fix potential vulnerabilities
22%
39%
44%
Don't have the funds to fix potential vulnerabilities
22%
33%
26%
Concerns about safety of the hack
22%
21%
13%
Could be embarrassing
22%
9%
4%
2005
2007
2009
0%
10%
20%
30%
40%
50%
60%
70%
Percent of respondents
N = 81
Note: includes only respondents who never conduct ethical hacks in at least one category, i.e., networks, operating systems or applications.

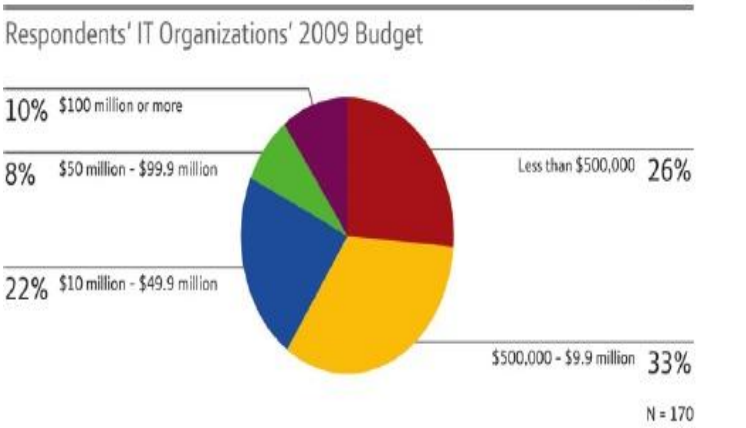

Ranking of Ethical Hacking Benefits
Improve overall security posture
43%
30%
12%
Protect against theft of intellectual property
22%
22%
11%
Fulfill regulatory/ legislative mandates
20%
14%
16%
Protect against possible lawsuits
4%
10%
14%
Baseline current environment
7%
6%
15%
Validate previous security investments
1%
10%
13%
Provide justification for additional funding
2%
4%
10%
Ability to do trending analysis
2%
4%
8%
0%
10%
20%
30%
40%
50%
60%
70%
80%
Percent of respondents
Top benefit
Second benefit
Third benefit
N = 125


Significant Barriers to Conducting Ethical Hacks Intenally or Improving Ethical Hacking Capabilities
Lack of experienced staff
53%
Other projects with higher priority
44%
Unrelenting introduction of new threats
41%
Cost of products/tools too high
40%
Amount of staff training required
39%
Justifying costs/benefits to upper management
35%
Organizational/process issues
31%
Difficulty in implementing products/tools
29%
Available products/tools don't meet requirements
23%
Lack of upper management support
20%
Staff turnover
17%
0%
10%
20%
30%
40%
50%
60%
Percent of respondents
N = 186
Note: includes only respondents who conduct ethical hacks using internal resources.









Challenges to Computer Security System

1. 80% of data loss is caused by insiders. 40% of Internet break-ins occur in spite of a firewall being in place. [18]
2. Increased Data Access
3. Larger User Communities
4. Data Tampering
5. Eavesdropping and Data Theft
6. Falsifying User Identities
7. Password-Related Threats
8. Unauthorized Access to Tables and Columns
9. Unauthorized Access to Data Rows
10. Lack of Accountability
11. Complex User Management Requirements

Prevent your system from Hacking problem:

1. The use of encryption of confidential business data, firewalls, e-mail monitoring, antivirus

software, security codes, backup files, security monitors, biometric security measures, computer failure controls, fault tolerant systems, disaster recovery measures, information systems controls, and security audits of business systems. [16]

2. Do not visit high-risk websites or click on any of the links there.
3. Avoid Scam/ Spammy Websites
4. Prevent illegal farmers' from "harvesting" your lists: Hacking techniques are used to "harvest" email addresses, which are then used by spammers and other hackers for malicious activities. If you are storing email data on your website, for what-ever required reason, make sure it's stored in a secure format, such as a MySQL Database.
5. Unsolicited Installation of Scripts: It can be dangerous to install third-party scripts and programs on your website unless you understand what they are actually doing. Even if you don't fully understand the programming, you can read through the code and look for tell-tale signs such as references to third-party URLS
6. Don't use Generic Usernames
7. Clear the Cookies!
8. Make sure your files are using the correct CHMOD Permissions: CHMOD File Permissions assign a specific value to every file/folder on your server, which allows different levels of access. CHMOD Permission range from 000 (No access) to 777 (Full access), you must decide which files get what permissions, but be warned that some third party software require higher permissions to operate properly. You need to balance out features with security and make an informed decision.
9. Use Strong Passwords!
10. Follow information security standard like ISO/IEC 27002
11. Updated Security Patches: If your web hosting provider hasn't already done so, you should check that all the latest security patches for various aspects of the service are properly installed. As you might know, WordPress (self-hosted) is one of the most popular Content Management Systems out there on the market.
12. Securing your Ports: ports are constantly opened & closed for easy-access, for programs such as a FTP (File Transfer Protocol). This can be favorable for any hackers attempting to access your sensitive files, so make sure any unwanted ports are 'properly closed.' [17]

Conclusion

Computer Hacking is threat to security system because directly or indirectly it may harm our system. There are many surveys done in past that proves many systems were hacked and they loosed their data or they their secure data is published and sold. We should keep a backup copy of your entire website and its databases. The use of software security software can improve system security. Still hacker may be improving them selves, and we should search for new initiatives in information security. People must be aware of the hacking so they can prevent hacking as far as possible. Ethical hacking is the best way to check security of system. Even separate budget is allotted to security system. We can recommend website developers to follow the three principles of information security: Confidentiality, Data Authentication, data integrity. They should follow information security standard like ISO/IEC 27002.

Let us learn from hackers, we should secure security system!!!

References:

1. http://ezinearticles.com/?Computer-Hacking&id=3369363
2. http://www.wisegeek.com/what-is-computer-hacking.htm
3. http://vickycomputerhacking.blogspot.com/
4. http://www.ehow.com/info_8660985_types-computer-hacking.html
5. http://ezinearticles.com/?Types-of-Computer-Hackers&id=3583931
6. http://en.wikipedia.org/wiki/Computer_security
7. http://www.theitlibrary.com/network-security.html
8. http://homesecuritysystem-10.com/computer-security-system/

9. http://www.ehow.com/facts_4965118_types-security-systems.html
10. http://signalnews.com/survey-hackin-businesses-466
11. http://www.securitynewsdaily.com/websites-hacked-government-commercial-cybercrime-2011-0556/
12. http://articles.cnn.com/2010-03-18/world/england.kids.hacking_1_hacking-survey-internet-cafes?_s=PM:WORLD
13. http://www.wright.edu/rsp/Security/V1comput/Threats.htm
14. http://www.acunetix.com/websitesecurity/web-hacking.htm
15. http://www.scribd.com/doc/23319524/Ethical-Hacking-Survey-2009
16. http://www.scribd.com/doc/396851/Security-and-Ethical-Challenges
17. http://www.blogussion.com/blogging-tips/ten-tips-to-prevent-hackers/
18. http://docs.oracle.com/cd/B10501_01/network.920/a96582/overview.htm

BY:

MS. PALAK PATEL

LECTURER, SEMCOM.

&

MS. HARSHIDA PATEL

LECTURER, SEMCOM.

My Voice:

Conquer Fear and Achieve Success

The biggest asset a person can have are intangibles like your thoughts, thinking process, attitude, outlook on life, intelligence which you can use to convert them into tangible wealth, property for the good of yourself and society and community at large. You may be less hurt by damage to your physical wealth but the amount of loss you may suffer due to damage to your intangible intellectual wealth in form of hope, optimism, dream, aspirations, efforts, vision, enthusiasm, morale and motivation is incalculable. The way in which farmer or gardener protect their produce from insecticides by applying proper manure, in the same way protect your thoughts, attitude, thinking, creativity, imagination, intelligence, foresight, vision, dreams, hope and aspirations to be corrupted by the negative thinking. The next question is how to identify negative thinking? It is really very easy to identify, when your mind tells you ten reasons for not doing any worthwhile activity, when it creates fear and uncertainty, it is negative thinking. Negative thinking and negative attitude with respect to your idea or venture is spreading the germs of negativity which will spoil your intellect, imagination, creativity and make you a loser. Healthy discussion on an issue or activity is welcome, but opposing the idea or activity without proper reason, logic, rationality is nothing but negativity.

The amount of loss which negative thinking can cause to your future success is huge. People with positive

attitude who believe in you and who encourages you by saying nothing is impossible for you are providing you the positive energy with which you were born. Most of the leaders, entrepreneurs, business executives, Chief Executive Officers share the trait of eternal positivity in their thinking, in their work, have clear vision, are not afraid or terrified by uncertainties and problems, and are extremely confident of the success of their ideas and business concepts. Dreaming big business or big worthwhile project and working smart and hard to convert your big dreams into reality is the hallmark of your success and achievement. The thing at the root of any economic progress, economic development, innovations, research and development is the insurmountable human urge to achieve impossible as impossible word breaks up as I-M-Possible for person with positive attitude. Moderate risk weighing benefits and costs can work wonders for the success of person.

So next time if you think that certain things are not possible, protect your thoughts from negative influence and tell yourself that you are the unique creation of almighty god with immense potentials and nothing is impossible against your strong will to achieve your worthy goals, dreams, aspirations. Truly for the creation of almighty, that is you, everything is possible. Negativity also gets spread by thinking that things are like this only, everywhere it is the same situation, we are helpless, we have no choice, and we have no options. The best way to deal with such negative thinking and resultant negative attitude is to ignore them and forget them forever. There may be situations where you may find below par performance receiving recognition, award and top notch work getting criticized and not getting recognition and prestige which it so richly deserves, but don't get demoralized. The belief and faith in god, guru and self can work to your advantage. So please don't restrict your dreams, aspirations, ambitions, as someone has rightly said what heart can conceive, mind can achieve. You do get positive energy by watching positive people, reading positive attitude literature, hearing melodious romantic positive songs full of energy, love, life, hope and which brings smile and cheer to your face and life. Think big, act big and achieve big, as size of your achievement and success does matter. In the ultimate analysis it is your attitude which will determine your altitude in life. So protect your attitude from getting poisoned by negative thinking and negative attitude. The small mantra for success and achievement is Think Positive and Act Positive. Let nothing stop you from the passion, determination, efforts you make to turn your worthy dreams into reality. It is rightly said behind every successful man there is women and blessings of almighty god and gurujii.

BY:

MR. SUNIL CHAUDHARY

LECTURER,SEMCOM.

.

ManageAnt:

Space Management or Space ManageAnt?

"Innovative businesses seeking a competitive advantage are looking to Virtual Offices to launch companies, test new markets and create new beginnings."

A number of elements must come together when we think about space. In today's era, it is very difficult to resolve Space or space management which is facilitated the implementation of a facilities master plan. Everywhere in any institutes, business world, any technical, physical or political we require Space and Space Management for establishing our institute or any such type of business. According to our task and goal we need to enhance our knowledge about the space which we require to fulfill our established goal or task. The first of these is a process to manage space and make planning decisions and secondly we need to focus on a clear set of institutional or business priorities on which planning decisions can be based. Thirdly, we can think about the budgetary approach.

Space management is the process or system of controlling the (total available) space (which can be free or used) for different purposes. The space management system (and thus the storage management system) guarantees ("promises") the space reservation.

Space Management assists in developing and adopting a space planning methodology that will the allocation and use of space resources. Space management ensures about the space allocation in an equitable and efficient manner on the basis of measurable need and approved standards of allocation of the space.

There are some general principles for Space Management which are as follow:

- To provide space as per the requirements that is appropriate and sufficient to support activities that are part of business activities or goals.
- For assigning blocks of space to the units for their use and proper management.
- Responsibility to manage the use of allocated space in a manner which responds to changing needs and demand.
- Reclaim and reallocated space as per changing needs and priority of the business or an institution.

So from the above idea about the Space and Space Management we can conclude that Space Management is like ManageAnt.

Looking forward!!!

BY:

DR. VIGNA OZA

LECTURER, SEMCOM.

Being:

Satisfied.?!

Each one of us might have cried on not getting first position in the class at one or the other time. That suggested that we wanted to be just first and not do our best that we can. Things remain the same throughout our life. We always want to achieve something we desire and not exactly we deserve. And if a person achieves the thing he desire, he will be satisfied. The word satisfaction is also unique. Life of this word is just for a minute or second. A student gets 93% marks in a subject, he'll be satisfied. Immediately he comes to know the news that, though he is not first in the same class. Satisfaction will lose its existence from there.

A person cannot be consistently satisfied in his life. It is said, "Don't be satisfied; otherwise you will not progress in life." Of course, if one be satisfied with the situation he is in, he will stop thinking for further aspects of life. To move forward, one need to be constantly unsatisfied, which he should restrict according to his ability and needs. About three years ago I read a book named: Who Moved My Cheese? In which the author wanted to say that for your food (job or progress) you may need to leave the place where you are. It is not only about the physical place but also about the growth of a person. One needs constant change in their level in order to progress in life. If your cheese is moved from a place, it means now it's time for you to move ahead and progress. If you be at your place and wait for your cheese to come. You'll wait forever or you may get the same sized cheese. But if you move in search of your cheese, there are chances of getting a bigger cheese. And when you go in search of a new cheese, you always try to find the bigger cheese that you find after considerable efforts.

Human beings have tendency to merge their own needs with some others' needs. We are often not satisfied because others got something and we did not. As I said in the beginning, we cried for not getting first in class. We felt bad because we did not get first and some other got. It starts with parents. Parents many a time compare their children with others not looking at their abilities. They might be good in some other areas but parents do not focus on those aspects of their children. It forces a human mind to be not satisfied by just seeing others' success and not their own failure. Human minds start developing this tendency, they start achieving something to defeat someone and not to win something. When your motive is changed of doing something, it does not remain with you for the longer time. If you have achieved a thing to defeat someone, then you have already defeated that person, you won't be consistent in achieving that thing.

It is true that satisfaction plays the role of a big hurdle in the way of your progress. Simultaneously; if you are not satisfied just because another has reached at a place and you have not, then your satisfaction becomes subjective. You are satisfied if you achieve something and not others. Before aiming for anything, one must look for the ability and capacity of ones. Because being satisfied with your own performance is more important than being satisfied with the position you get no matter, what performance you give.

BY:

MR. DIPEN BHATT

Lecturer, SEMCOM

Green Corner:

AN INITIATIVE By SEMCOM:

GREEN BUSINESS EXHIBITING COMPANIES TAKING AN INITIATIVE TOWARDS PROTECTING ENVIRONMENT THROUGH PRODUCT/PROCESS

Companies were selected on following criteria

- Companies are redefining their business practices due to Climatic Changes.
- Awareness about Carbon Credits
- Encouraging in reducing GHG's. (Greenhouse Gases).
- Awake the public about using Renewable or Recyclable products.
- Importance of 3 R'S: Reduce, Reuse & Recycle.

SUZLON

Suzlon provides 'End-to-End Solutions' for the Indian markets in the wind power domain. From initializing a project, till completion and beyond, Suzlon offers solutions at every stage of wind-powered energy.

GFL Windfarm

The GFL Windfarm is a 23.1MW renewable energy wind-farm in Gudhepanchgani in the state of Maharastra India. Operational from April, 2007, the wind farm is made up of 14 wind turbines each capable of generating 1.65 MW of energy and displacing 51,618 tonnes of greenhouse gas emissions caused by the burning of fossil fuels.

Emeral Energy Solutions Pvt. Ltd.

Emeral has core expertise in Solar PV and Solar Thermal Solutions. They have mapped the industry need and designed highly economical innovative solutions to serve the exact need.

Daman Ganga

Daman Ganga is a company engaged in recycling packaging products with a focus on environment friendly technologies. A recycling of tetra pack products is done to make roofs, bathrooms, furniture & many more.

Kribhco Fertilizer Ltd.

Kribhco diversified in to the field of Bio-Fertilizer in the year 1995 in order to provide supplementary nutrients at low cost to the farmer.

SAHAJ

SAHAJ is a fair trade organization and it takes care of environment as its principle of organization. To help farmers and rural people, SAHAJ has taken this initiative which helps people to earn livelihood as well as it also help to protect our nature and environment.

ABELLON CLEAN ENERGY Abellon clean energy is an integrated sustainable energy solution provider with a vision to contribute to clean energy generation through focus an bio-energy including bio-pellets and other forms of clean energy generation

AURA HERBAL TEXTITLE LTD. eliminates deadly chemicals from your clothes & textile as well as from environment, which ensures a sustainable life for the global community.

SOLUTIONS FOR ENERGY PVT LTD. is committed to provide energy solutions that are green, clean, cost effective, rewarding and most suited to the

individual application s. We aim at the business we operate.

GUJARAT NARMADA VALLEY FERTILIZERS COMPANY LTD.

GNFC Today has extended its profiles much beyond fertilizers through a process of horizontal integration. Chemicals/Petrochemicals, Energy Sector, Electronics/Telecommunications and information

Technology form ambitious and challenging additions to its corporate portfolio. GNFC has an enterprising, strategic view towards expansion and diversification.

INDUSIND BANK

IndusInd Bank will reduce the carbon footprint by 1942 kgs of Co2/every year for next 20 year. The solution is an effort to go green with technical and

financial viability.

WARM STREAM

Warm stream offers an excellent distributor/dealer program which can be further customized to individual company requirements.They export steam Boilers, thermic Fluid Heaters, Chemical Process Equipment and complete plants on turnkey basis.

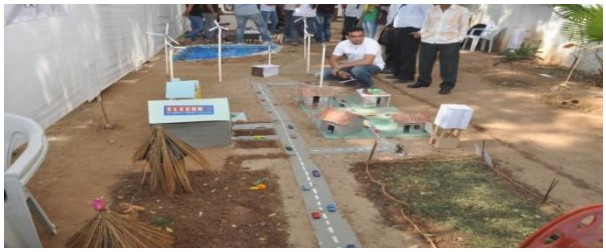
SUPERNOVA TECHNOLOGIES PRIVATE LIMITED.

Supernova Technologies Pvt. Ltd. has achieved highest number of installation of windmills in the country and that too without subsidy. Company manufacture as per the need of clients (Tailor made solution). These Wind Generators are developed indigenously as per Indian Environment and Requirement.

NESCO LIMITED: INDABRATOR DIVISION Product: - JET-3 DUST COLLECTOR

JET III is a wholly new design in pulse JET dust collectors, offering the high collection efficiency by increasingly stringent environmental regulation, plus true economic is achieved by a new state of The art system designed to reduce maintenance, labor, parts and energy cost.

ELECON



As per the present study and situation, Wind Power installation is growing at a rapid pace worldwide and expected to maintain high levels of growth rate in the next 10 years. More as a part of initiative Elecon has taken an opportunity to help the world in reducing the global warming by providing the solution to generate the GREEN POWER by harnessing energy through renewables, mainly through wind.

BY:

MS. HIRAL PATEL

LECTURER, SEMCOM

Contributors:

"DRIVE" is regular monthly e-news letter published by **SEMCOM**. This e-news letter deals in all aspects of management, commerce, economics**,** technology and Humanities. It is open for all students, alumni, teachers and professionals dealing with above stated areas.

Your contribution in the form of research papers, articles, review papers, case studies are invited for publication. All papers received by us will be published after the approval of our Editorial Team.

You are requested to send your article to kpatel@**SEMCOM**.ac.in

OR

mail at:

SGM English Medium College of Commerce & Management (**SEMCOM**)

Opp. Shastri Ground
Vallabh Vidyanagar - 388 120
GUJARAT
INDIA

Tel. No. : +91 2692 235624, 231811
Fax. No. : +91 2692 235624