Corporate social responsibility and business ethics assignment

Art & Culture

Completion of this project within the limited time frame would be impossible without her continuous support and guidance. Tuned Declaration This is to certify that the Research work incorporated in the report " Ethical and Unethical Hacking" a Boniface work done by Nikkei Aurora, Irvin Tambala's, Kayaks Manikins, Deviant Dossal and Nikkei Shoat. This work is submitted in partial fulfillment of the requirement for ABA degree in the academic year 2013 – 2014. SIR. NO TOPIC Literature Review 2. Hypothesis 3. Objectives 4. Introduction 5. Primary and Secondary Data 6.

Conclusion 7. Bibliography 1 . Dry. B. Intramural is his article cybercaf?? scenario in India mentions that " Cyber-crime is emerging as a serious threat. World-wide governments, police departments and intelligence units have started to react. Initiatives to curb cross border cyber threats are taking shape. Indian police has initiated special cyber cells across the country and have started educating the personnel. This article is an attempt to provide a glimpse on cyber-crime in India. " Link: http://www. Gal.. In/downloads/BMW_cybercaf??. PDF 2 Mr..

Renal Nana In Nils article correctly vs. corollary- It Is Just A Beginning mentions that " The genesis of internet was initiated by Vinson Cert. who first developed what later became known as the ' internet' I. . The interconnectivity between computers worldwide in the year 1973. Few years later, on 25th of December 1990, Tim Burners-Lee with the help of Robert Claudia and a young student at CERN (Concise Europe?? en pour la Recherch?? Uncle?? Eire) invented the World Wide Web (www) and implemented the first successful communication between a Hypertext Transfer Protocol (HTTP) client and server via the internet.

The founding fathers hardly had this notion that internet could transform itself into an all pervading revolution capable of being misused for criminal activities, if fallen in palpable wrong hands of the evil elements in the civilization and which required regulation. Today, where the know-how of internet has become immensely popular and easily available, added as a subject for studies in educational institution in every society all over the globe, being used by corporations and governments, hospitals, military, and by almost all individuals and organizations in the world.

It’s because of its efficiency and usage in all matters providing flawless results and products, that has led to internet’s extraordinary growth and dependence since the day of its invention till today, which is a shockingly short time for such a success. Internet has induced a rapid growth in all the sectors and has changed and affected the human civilization massively making their life easier leaving its mark. In the present time, which is also called the digital age, many disturbing things are happening in the cyberspace.

Due to the anonymous nature of the internet, it is possible to engage into a variety of criminal activities with impunity and people with intelligence, have been grossly misusing the aspect of the internet to perpetuate criminal activities in cyberspace. Hence the need of cyber laws in India. ” Link: http:// www. Manufactures. Com/articles/Penetration. Asps? Old= Beebe- dc AAA-Bcc-off-c IEEE baobab RCA u information techooenologyCyber Lalaw

Christopher VersVersahis article 2014sass’sking Pain is Cyber Security’s Gain states that “ Let’s face it, cybecybercaf?? an exploding pain point for many

and it’s given rise to not only privacy concerns, but boosted demand for cyber security. In late 2012, Defense Secretary Leon PanePenetratened the US would likely face a “ Cyber-Pearl Harbor” and the country was increasingly vulnerable to foreign computer hackers. Per PanePenetratekely targets included the nation’s power grid, transportation system, financial networks and government.

CybeSubjectivityvider McAfMacAfeeich is a wholly owned subsidiary of Intel INTCINTO 9%, sees the pace of cyber attacks only accelerating in 2014 compared to 2013 and 2012. From mobile malwmallardpecially on Google GOOGAGOG 53%’s Ag’sroid platform, to the continued rise in cyber-criminal gangs that will target enterprises and the likelihood that social media attacks on FaceFaceablenkLinkedDLINK 2%, Google+, Twitter (TWTRTRWd others will be ubiquitous by the end of 2014 the McAfMacAfees 2014 Threat Predictions eporporterscores PanePanatela’s2 warning. ” 4.

PavaPaeangDugganhis article the face of Indian cyber law of 2013 states that “ Indian cyber law is still ineffective in aellleveringecoyermcremevconvictionsen as cyDecideruTraumatcontinuesIncrease The year 2013 has seen a lot of events as far as cyber law Jurisprudence in India is concerned. It has been an eventful year that demonstrated how cyber legal challenges are increasingly becoming relevant. The CMS, SMSe news of which came in post SnowSnowmenelations, is supposed to be an omnipotent system for monitoring, decryption and surveillance and has immense apacopacitiescarry out surveillance of audio, video, image or text.

The CMS SMSught to the forefront the complex challenges pertaining to its legality and also its direct infringement upon people’s fundamental right to privacy as enshrined under Article 21 of the Constitution of India Given the fact that CMS SMSs far beyond the accepted norms of surveillance, monitoring, interception and much beyond the scope of Section 69 of the Information Technology Act, 2000, it is thus clear that CMS SMSs not really fall within the ambit of the limited permissible circumstances of monitoring, interception, decryption and locking as detailed under Section 69, 69A AAAthe Information Technology Act, 2000.

As per the Google’s Transparency Report, 2013, in the case of India, the number of user data requests rose by 16 per cent to 2, 691 in January-June this year from 2, 319 in the same period in 2012. ” Government considers hacking as a cyber-activity and not a crime when it’s authorized by them. 1 . To understand the Advantages of Ethical Cyber activity vs. vs. etUnethicaler activities (cyber-crime) 2. To understand how institutions (Government Organizations) use hacking as a tool for recovering lost data and if this is ethical? To understand how cyber-crimes in some cases are condoned as ethical. Ethical and Unethical Hacking have been in debate for nearly half a century. But each definition differs from one another in all aspects. A white hacker is someone, who is known as a Good Guy, but a black hacker is considered as a Bad malicious attacker. Overall, the debate seems to more inevitably a moral issue of wrong and right and wrong. Though many of us are really confused between these two terms but still, at some point we do understand the benefits and curses coming with hacking.

But any of us tend to be confused between the concepts of Ethical and Unethical Hacking. To us, hacking is itself, automatically called as Unethical or illegal. Normally, hacking can be defined as unauthorized breach of barriers put for the protection of important data, information and people as well. Initially hacking was all about breaking laws and accessing unauthorized information by certain groups of people, specializing in Information Technology and Computer Programming.

Some of the major computer companies such as Apple, IBM and Microsoft comprises of large team of dedicated, talented and professional hackers. These hackers, however are not breaking the laws, so far nobody can tell. For an ethical hacker, their Job includes to test the newly developed program to find loopholes in security system of the program. In simple words, an etnltentacleKknackersa computer expert, wno wonacks a highly protected security system on behalf of his owner with care and prevents the exploitation of the program that an unethical hacker might cause harm.

In order to test the program, ethical hacker makes use of methods as their less principled counterparts but unethical hacker utilizes each resources and opportunity available o create malicious attack the security system. On other hand, an unethical hacker is more of a vigilante, who is basically involve in exploiting security vulnerabilities for some hackhastiestperson who wants to get unauthorized access to the system. The technical differences between Ethical and Unethical Hacking is ZERO, but what counts here is Moral difference, which is substantive.

At present, most of the companies have their own hackers. Both the hackers seems to do well in their business, depends who hires them. It can be well termed as the fghtfightween Police Force and Criminals. Still, the debate will continue to go on for Ethical and Unethical Hacking forever. Primary and Secondary Data collected There are two types of data. They are primary data and secondary data. Both primary and secondary data illustrates the gathering of information and to satisfy the goals of business. Primary data is nothing but it is the data which is collected newly and for the first time.

The primary data is original. It is the fresh data and is never gathered before. Secondary data is the data which is collected by others. The data is collected from newspapers, magazines and Journals. Secondary data is gathered before primary data since it is time consuming. Data is gathered newly in case of primary data so it takes much time. In this Research paper we are using Secondary Data. Ethical hacking: bad in a good way 17 December 2012 By AashAishahBoyhoode and more orgaorganizations being targeted in cyber-attacks, and they must get to know their enemy if they are to protect vital networks.

Meet the professional, ethical hacker. Nasty, evil, devious, manipulative: adjectives commonly planted in front of the term ‘ hacker’. But stick the word ‘ ethical’ in front of it, and you may Just ave eveuck on a useful concept. Of course, ‘ ethical hacker’ sounds like an oxymoron: how can such a disruptive, destructive coder ever lay claim to a code of ethics? With tne tene 0T cATecoyermcremenltentacleKNanking NASoDecodeowepowerfulategy In tne tennTalentinst online threats.

In general terms, ethical hackers are authauthorizedbreak into supposedly ‘ secure’ computer systems without malicious intent, but with the aim of discovering vulnerabilities in order to bring about improved protection. Sometimes the local IT managers or security officers in an orgaorganizationl be informed that uch suchattack – usually called a ‘ penetration test’ – is to take place, and may even be looking over the hacker’s shoulder; but often they are not, and knowledge of an attack is confined to very senior personnel, sometimes even Just two or three board members.

Some ethical hackers work for consultants; others are salaried staffers, who conduct a scheduled progprogrammerhacks on a regular basis. A number of specspecialistsst within the general discipline of ethical hacking; for this reason it is impossible to group all ‘ hackers’ into a comprehensive category. An ethical hacker, lso alsoerred to as a ‘ white-hat’ hacker or ‘ sneaker’, is someone who hacks with no malicious intent and is assisting companies to help secure their systems.

However, a ‘ black-hat’ hacker is the opposite and will use his or her skills to commit cybecybercaf?? spically to make a profit. In between are hackers known as ‘ grey-hat’ hackers, who will search for vulnerable systems and inform the company but will hack without permission. Tools of the raid trade Ethical hacker Peter Wood, founder of penetration-testing vendor First Base Technologies, specspecializesWindows networks and social engineering. His first ‘ packet sniffing’ exercise was in 1978, when he worked with defedefenseporation Raytheon, and later tested IBM’Vim’swork systems.

The choice of tools used depend on the task, says Wood, but when testing a corporate Windows network he will use Hyena – a program designed for Windows admiadmits programs fgdufudged SAMIAssassins Windows password-cracking. He adds program Core Impact is ideal for running exploits as it creates a solid audit trail. Cyber security issues change every day – new viruses, new malwmallardw ways to crack through even the most robust online defedefenses

The threat landscape' has grown out from simple password breaking, viral infection, and the exploitation of weakness in online access safeguards, through to cyber-espionage, data asset theft, and denial of service (DOS) attacks. Add to this the proliferating problem of ' hackhucksterismthe deployment of hacking techniques as a means of protest to promote political ends. As well as the external baddies, orgaorganizationsall kinds are continually challenged to adopt emerging digital information technologies, such as bring your own device (BYODBOYDd cloud computing, which bring their own security issues.

Now however businesses are facing increasingly accurate and sophisticated attacks. Despite spending millions implementing firewalls, anti-virus/anti-malwmallardtware, hardware firewalls, and data protection applications, there are still flaws in many orgaorganizations security perimeters, and it's not necessarily the fault of the security technology. This has resulted in companies employing ethical hackers to perform penepenetrationts, vulnvulnerabilityns ana Ana alanTyler tennown .

EtnlTentacleKknackers be deployed to look for vulnerabilities from both inside and outside an rganorganizationvert cyber criminals can pass themselves off as bona fide employees to conduct their nefarious ends from within corporate premises. Hacker History In 1974, the MultMulticastltiplexed Information and Computing service) operating systems were then renowned as the most secure OS aSOilable. The United States Air Force orgaorganized'ethical' vulnerability analysis to test the MultMulticastaSO found that, though the systems were better than other conventional ones, they still had vulnerabilities in hardware and software security.

As companies begin to employ thicethicalkers, the need for IT specialists with accredited skills is growing, but ethical hackers require support too. Shortly after the 11 September 2001 terrorist attacks on the World Trade Center, Jay BaviBasis HalaHalliUnhiddenfounded the International Council of Electronic Commerce Consultants (Ec-cSecncil), a professional body that aims to assist individuals in gaining information security and e-business skills.

Government institutions have recorecognized benefits in using ethical hackers; the problem is where to find them. In 2011, UK intelligence agency GCHQECHOnched ' Can You Crack It? , an online code-breaking challenge in the aim to recruit ' self- taught' hackers to become the next generation of cyber security specialists. Early in 2012 GCHQECHOo unveiled a cyber-incident response (CIR)CIRRIlot scheme.

This initiative launched by the agency's Communications-Electronics Security Group (CESGCUESd the Centre for Protection of National Infrastructure

(CPNICHIPill provide a range of support from tactical, technical mitigation advice to guidance on the use of counter-measures to improve the quality of security within the public sector and critical national infrastructure orgaorganizations present, data-intelligence provider BAE BABEtems DetiDedicate security providers CassCustodianntext IS, and MandMaintaine been selected by CESGCUES CPNICHIPwork in partnership to provide support.

A GCHQECHOkesperson revealed both GCHQECHO CPNICHIPe not incurred any additional costs in establishing the scheme, but in line with other certification schemes they will charge an annual certification fee when the CIR CIRRIeme is launched in 2013. “ We certify ‘ ethical hacking’ companies ourselves to undertake penetration testing of government IT systems, and work with industry schemes CREST and TIGER in setting the right tandtankards these companies to work to,” adds a GCHQECHOkesperson. How etnltentacle’etnltentacle

Even though more enterprises are actively recruiting ethical hackers, for some there remains a hesitation when it comes from letting a licensed attacker loose on corporate information systems. According to the report When is a Hacker an “ Ethical Hacker” – He’s NOT’ by AlieAlienist’search engineer Conrad Constantine, an ‘ ethical’ hacker simply does not exist, and it is the contradictory Job title that is the problem. “ The term ‘ ethical’ is unnecessary – it is not logical to refer to a hacker as an ethical hacker’ because they have moved over from the ‘ dark side’ into ‘ the light’,” Constantine argues. The reason companies want to employ a hacker is not

because they know the ‘ rules’ to hacking, but because of the very fact that they do not play by the rules. ” Constantine adds: “ Some hackers would argue that they’re not criminals, but activists. Others would say that they’re Just rebellious in the way they think about technology and have a duty to highlight an orgaorganization’sr security. My personal view is that we need people who are willing to stand up and challenge authority – in o doing, does that then make them ethical?

I dontdon’t why it should, it is still hacking – end of argument. ” Supporting this, FaroBaroniesject management vice president DmitDimitysSteerings: “ Have you ever heard of an ethical hacker that has started off as an ethical hacker? I have not. ” “ Experts do not typically adhere to textbook coding practices, and can uncover problems, vulnerabilities, or business practices of varying shades of ‘ ethical’ – something they were not supposed to uncover,” adds ShesSteeringo the concern often remains, how ethical is an ethical hacker? ” Turning tables