Cyber Security Scenarios and Control for Small and Medium Enterprises

Nilaykumar Kiran SANGANI[1], Balakrishnan VIJAYAKUMAR[2]
[1]M.E. (Software Systems), CS Dept., BITS Pilani, Dubai Campus, Software Engineer with Emirates Group IT
[2]Associate Professor, CS Dept., BITS Pilani, Dubai Campus
sanganinilay@hotmail.com, vijay@bits-dubai.ac.ae

As the world advances towards the computing era, security threats keeps on increasing in the form of malware, viruses, internet attack, theft of IS assets / technology and a lot more. This is a major concern for any form of business. Loss in company's status / liability / reputation is a huge downfall for a running business. We have witnessed the attacks getting carried out; large firm's data getting breached / government bodies' sites getting phished / attacked. These huge entities have technology expertise to safeguard their company's interest against such attacks through investing huge amounts of capital in manpower and secure tools. But what about SMEs? SMEs enrich a huge part of the country's economy. Big organizations have their own security measures policy which ideally is not applied when it comes to a SME. The aim of this paper is to come out with an Information Security Assurance Cyber Control for SMEs (ISACC) against common cyber security threats implemented at a cost effective measure.

Keywords: *Information Security, Cyber Threats, Small and Medium Size Enterprises, Security Threats*

1 Introduction

Over the past few years we have seen the increased growth in the field of Information Systems. SMEs are making a huge presence in the field of Information Technology to mark their footprints within the technology network. Implementation of new technology systems has changed the way SMEs running their business. They are able to raise their market presence and contribute into the ever growing economy of the country [1]. Adopting new technology to achieve goals in any large organization or a SME without considering the open risks – to name a few - such as malware, data breaches, unsecured network leads to unreliable outcomes in the business [2]. Huge organizations can always protect themselves by designing and implementing highly tested security policy solutions. Whereas the same to be implemented in a SME can lead to various problems because such bodies/enterprises are shortage of specialized security technical architects/implementers to design and highly maintain such required solutions [1], this can be due to budget constraints or IS security is not their primary concern as they say - "After all, who would want to target my business when there are so many bigger targets out there" [3].

Internet has become the most important asset for SMEs for their business. They need to be connected throughout for their success which makes their systems/assets/human factors highly more vulnerable for an attack. Majority of Small and Medium business feel that IS Security is not their main concern. Preemptive measures are been addressed for the new emerging threats in the market. Still, SMEs do not consider protecting their business for few of the reasons as highlighted earlier. In most of the situations we find SMEs are not clear in their steps to implement such cyber security control mechanism [3].

Profits and Company's brand growth are primary factors considered for a successful business. Pertaining to SMEs if any one of the above mentioned factors are compromised – their growth and reputation is hampered. Their systems are compromised leading to Data theft/or an insider leaking out the company's secrets/or their sites have been brought down through a DDOS attack/ or viruses/malwares have been planted in their

network will lead to major downfall in their customers trust if IT Security control measures are not implemented effectively to mitigate such risks[4]. Main priority for SMEs is to keep their business verticals aligned with their Mission & Vision which in turn they find it difficult to in-corporate secure process in them. This paper is organized as follows: Section 1 is the Introduction. Section 2 talks about the motivation in order to bring out this paper. Section 3 focuses on Cyber Security Threats and their counter measures. Section 4 brings the conclusion and future work.

2 Objectives and Motivation

In today's global economic situation SMEs heavily depend on the Internet/Information Technology to showcase their expertise/products/solutions. They create an employment opportunity which in turn generates profitable income. When it comes to multitasking, they are very well balanced set of enterprises. They are heavy suppliers for major sectors, their inner business approval decisions takes places very fast, very quick in making critical decisions and very flexible to amend their structure with any given business requirement. But when it comes to IT Security, we often come across SMEs lack the technical expertise, the funds, the knowledge, and security architects to protect their systems against cyber threats, create organizational policies & tasks pertaining to Information protection [5], [7], [8].

The management of a SME does not see their company as a liable target for cyber crime attackers or hackers. Most of their managers think to implement IT Security is just to install an anti virus or implement a firewall which is an incorrect misconception thinking that cyber security issues are just meant for large organization(s).Online Information processing and dependency over the Internet are growing at a fast rate which has become the prime issue for enterprise information security. Most of the SMEs depend on their Information Systems/Internet for their various business activities without even knowing of how to secure their information/data from attackers/insiders/disgruntled or ex-employees [7] [8].Very few SMEs have their own IT Security implemented but at a very minimal cost as investing in protection of their Information System is not their main concern until unless an attack is carried out on them [8].

In today's environment, cyber security threats and weaknesses in the information systems/assets are the major hurdles faced by SMEs without their implementation of IT Security policy & procedures, data protection mechanism etc. In the absence of such measures – it leads to manipulation/loss/modification of data, internal theft of the assets etc [6].The users/customers of a SME always have a high impression that their sensitive data is protected under the best security mechanisms. Large firms/organization who does business with the SMEs wants to be assured that their huge data which are flowing in and out of a SME are not breached. If the protection fails, can result in loss of the customers trust, monetary loss and there can be high chances of fines/penalties from legal authorities [9]. It is very much necessary/essential to protect information (such as software, hardware, management controls).There is always a cost involved in not protecting information.

Securing information from the cyber attacks is the most common and primary aspect of all stakeholders. The crux of any Information security systems are the budget cost linked with its design, development and implementation [2].Huge investments needs to be carried out in building a highly reliable cyber security solution. SMEs operate totally different from huge organizations. They do not implement the cyber threat control system found in multi-organizations like Policies, security professionals & managers, IS Auditors etc. Within an SME environment, IT Security needs to be implemented taking its limited resources and budget into consideration. It was found out that at least half of the SMEs were not using the most common and elementary cyber security protection of implementing anti virus programs. Keeping the former into consideration, cyber attackers have increased their attacks more towards

these small and medium businesses as they are easy targets [10].
Most of the SMEs turn a blind eye to IT Security. As Per [12], they are under "if it's not broke, don't fix it" attitude. Having the expertise also within their organization, they never budget on implementing cyber security solutions to protect their information/assets. A rapid example would be the "Here you have" worm. As per Symantec, it was listed as a "malicious computer worm using a socially engineered email attack". This worm was delivered via an e-mail integrated in a PDF file luring the users to click on the PDF link, which, which clicked downloads a program that disables the antiviral programs and performs many more actions [11].Looking into the above, SMEs should be aware and conduct various security awareness trainings and make their employees aware of such situations which due to their action could cost their business a fortune. Cyber security threats and its vulnerabilities demand a very deep understanding as how the attacks have been originated and how to prevent the attack from occurring. Such insights will help the SMEs towards their implementation of the protection controls which will assist them to identify and mitigate such threats.
Our contribution in this paper is to bring out *an Information Security Assurance Cyber Control for SMEs* at a cost effective measure. The advantages of this to a SME will permit them to – a) Understand & Identify Cyber Threat attacks and their vulnerabilities. b) Mitigate & prevent by providing counter mechanism for such attacks.

3 Cyber Security Threats

Over the past few years, there has been tremendous increase in the cyber threats due to penetration of new and high end technologies within the global economy as it involves heavy usage/dependency of the Internet to carry out businesses for personal/business/government sectors [13]. SMEs have been using Internet as one of the primary medium for to showcase their businesses to the new and existing users. In parallel – Various new threats are emerging to hamper such businesses [14].
In this section, the most common cyber security threats for a SME have been studied. How these threats originate and what are the steps taken to mitigate such threats will be covered which will ensure continuity in the business, maintain users/customer privacy and reduce the business/execution/operational costs.

3.1.Phishing

One of the most structured cyber crimes of the 21st century carried out by the attacker [16]. According to The United States Department of Justice defines phishing as " 'Criminals' creation and use of e-mails and websites – designed to look like e-mails and websites of well-known legitimate businesses, financial institutions , and government agencies – in order to deceive Internet users into disclosing their bank and financial account information or other personal data such as usernames and passwords"[16].

3.1.1 How you become a victim of Phishing?

You have received an e-mail from your bank's credit card section informing that your account has been cancelled/de-activated due to an upgrade in their systems or they have encountered a suspicious activity going around your account or for an audit activity taking place. The very same message directs you to click a link back to their web site and requests you to enter your bank account details and credit card details in order to verify that you are a legitimate customer and they can once again activate your account. Details can be in the form of but not limit to your username, password, account no, social security no., pin no. etc. The website which populated by clicking on the link seems all proper and in-place. The logos/fonts look proper, the website address looks real and convincing and the layout of the site is the same since the last time you have logged in. You think it is your bank site as everything is just similar. The catch is - the e-mail is not legitimate, the site is a replica of the original one. Once feeding in the information in the fake site –

the cyber attacker has all of your information. You have been phished. You have fallen and became a victim of one of the most so called organized cyber crime called 'Phishing' [17].

3.1.2 Typical Phishing Attack

Figure 1 depicts a typical phishing attack.

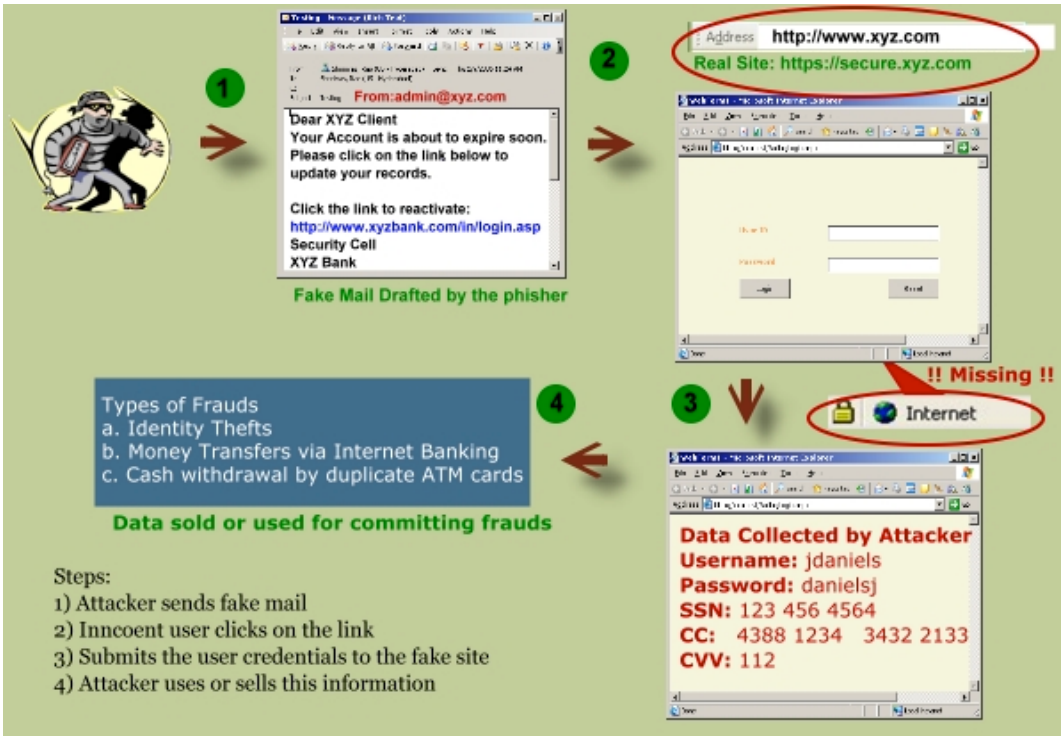

Fig. 1. Phishing Attack
Courtesy of SANS Institute InfoSec Reading Room [16]

3.1.3 Recognizing a phishing scam in an email

As per Microsoft Safety & Security Center [15] – below is an example (Figure 2) to see recognize a phishing scam in an e-mail message:

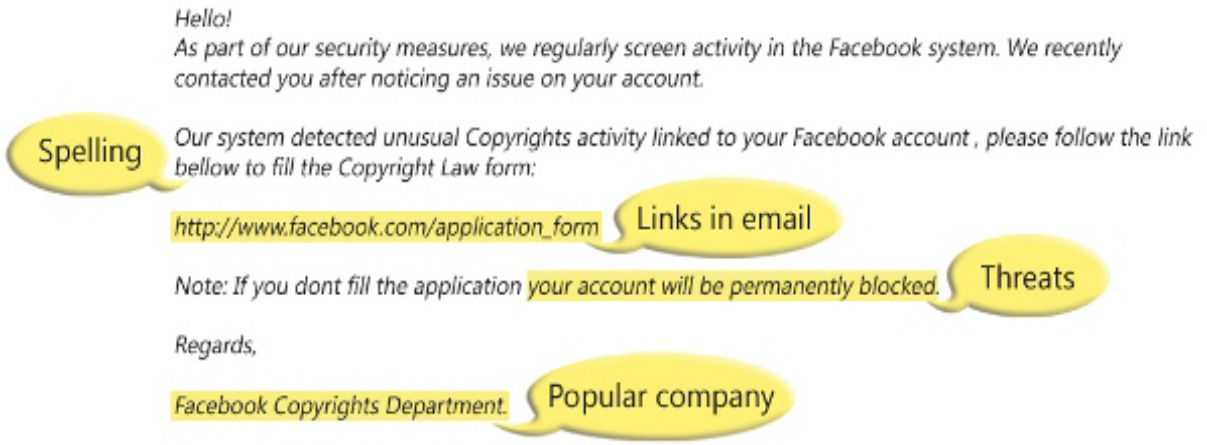

Fig. 2. Recognize a phishing scam
Courtesy of Microsoft Safety & Security Center – Computer Security, Digital Privacy and Online Safety [15]

Factors to be looked at to identify a phishing scam [15]:

- *Bad Grammar and Spelling*: Big firms/Service providers/Financial Institu-

tions will never make a spelling mistake or a grammar error in their sentences. They have their own staff to proof read or automated programs to recognize if any such errors within their constructed sentences. But when it comes to cyber attackers – they are not so good in grammar and spelling. Even if they make a mistake, they do not mind because that is not their motive. So if you come across such mistakes in an e-mail, there is a high possibility that might be a phishing scam mail;
- *Threats*: Receiving e-mails such as your e-mail account/back account/social networking account etc. is going to be blocked if you do not click on the link mentioned, depicts to be a form of scam related content. Suck fake alerts do contribute to identification of a phishing scam related e-mail;
- *Watch out for links in e-mail*: Do not click on links within the e-mail which you feel the content is not legitimate. Move your mouse over (but do not click) the link to check if the address matches to the link which was embedded in the message. In the below image (Figure 3) – we see the link highlighted in yellow showcase the real web address which doesn't matches with the original one in blue;

Fig. 3. Link in yellow showcases the real web address
Courtesy of Microsoft Safety & Security Center – Computer Security, Digital Privacy and Online Safety [15]

- *Replication & spoofing of popular websites*: Cyber attackers in their scam e-mail uses similar logos/fonts/or content of the original website and lure the users to click on them which takes them internally to some scam related sites or might even open up a pop-up which might internally perform some ill-related functions such as download an .exe files which might contact a virus some malicious software;
- *Cybersqatting*: At times cyber criminal uses web addresses which are pretty much similar to the original domain web address or they are in the form of wrong spellings of websites. For E.g.: If we take www.microsoft.com – Cyber attackers might create something like : www.micrsoft.com/www.micosoft.com/www.mircosoft.com

3.1.4 Control measures to avoid phishing

- never reply to any e-mails which requests account information/personal information/ or to confirm the very same. Either e-mail or call the very same company who has requested to information to find out if the e-mail is send by the legitimate source [17];
- if you feel the content in the e-mail is not legitimate but has come from a legitimate source, call the direct concerned person or the organization from where it seems the e-mail to have come from before performing any activity in the e-mail such as clicking the internal links or replying back [19];
- in Internet Explorer – the domain name in the address bar will be in black and the remainder of the address will be in gray – making it very easy to infer that the website's true identity[20];
- install Smart Screen Filter as it is a feature in Internet Explorer which helps detecting phishing websites [20];
- always use a secure website when submitting personal/sensitive/credit card information over the Internet (Web Browser) [21];
- these days' phishes are able to spoof/replicate websites and make them start with https:// that we see on a secure web server. To be more careful – always type the address of any financial/shopping etc website by yourself ra-

ther than clicking on the displayed links [21];
- install a web browser tool bar to protect yourself from scam/fraud websites. Such tool bars will match against the list of known phisher sites and if found anything suspicious, will alert you. Internet Explorer and Firefox provide such toolbars [21];
- make sure your browser is patched with the latest updates [21].

3.2 Web Application Attacks

To increase the profits in a business, companies adopt the strategy to market their products and services through the internet. Hackers are always on the prowl to find a vulnerability in these sites which helps them to launch their attacks either targeting the corporate or the end-users. The most common and frequent web application attacks are launched via SQL injection attacks and cross-site scripting (XSS).In recent years big giants like Facebook, Twitter & Google Analytics had major issues in XSS [24]. These attacks are originated because of coding errors and inputs/outputs of an application are not sanitized [22]. In the Figure 4 below, as per the Web Hacking Incident database (WHID) for 2011 it depicts that SQL Injection and XSS are the most famous hacking techniques [26].

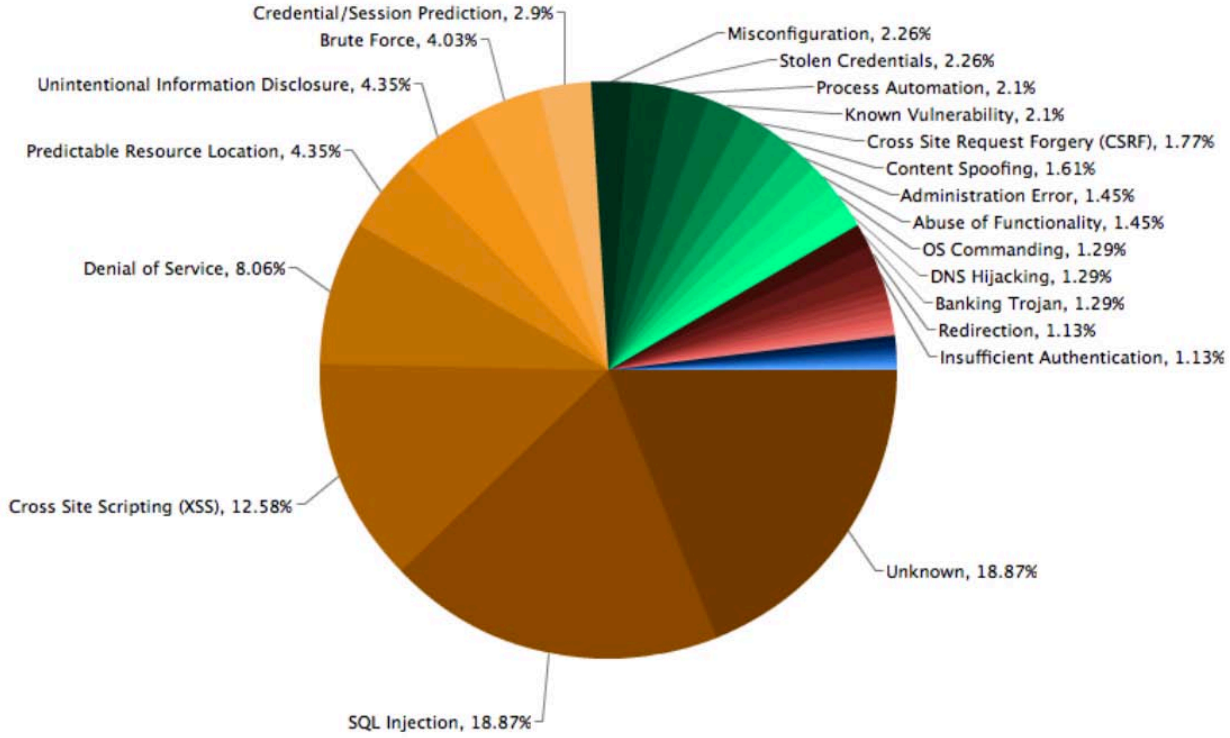

Fig. 4. Web Hacking Incident database 2011
Courtesy of www. http://www.acunetix.com[26]

3.2.1 How you become a victim of SQL Injection?

SQL Queries are inserted through the input fields via the client to the application. This allows the attacker to execute queries/commands in the application's database to tamper/delete/destroy the data. Queries can be executed to amend the privileges of the server.

3.2.1.1 How SQL injection does looks like?

Assuming C# as the language in the following example and 'phone.Text' is the input text field in your application. Consider typing the following text '; DROP DATABASE testabc -- in an input text field in your application where it expects a number.

Select testname, testaddress from testdb

where phoneid= '"+phone.Text+"';
The developer has written the above statement in order thinking user is going to input a number which will look like *Select testname,testaddress from testdb where phoneid='12345678';*
But as the user has inputted '; DROP DATABASE testabc, the select statement therefore will look like

Select testname, testaddress from testdb where phoneid= "; DROP DATABASE testabc --'

From the above statement we infer, the '(single quotation mark) which is the starting character of the scamp input will terminate the preset string character in the SQL statement. This will close the present statement. Thus, the opening of single quotation mark character of the scamp input will give the output as

Select testname, testaddress from testdb where phoneid= ' '

The ; (semi-colon) character will convey the SQL statement that it is the end of the present statement thus making path to execute the wrongful SQL code.
Note: Some database providers does not require semi-colon to separate SQL statements. It depends once again on the way it's implemented.
The - - (dual dash) character is a form of a SQL comment to convey the SQL to ignore the rest of the code. In the above scenario, it will ignore the '(single quotation mark) which will cause a parser error [23].

3.2.1.2 Control measures to avoid SQL Injection attack

-**Sanitize input data**: Input data should be validated and checked before submitting the page;
-**Use type-safe SQL parameters**: These parameters can be used either with Stored Procedures or dynamically created SQL command lines.

3.2.2 How you become a victim of Cross Site Scripting (XSS)?

XSS originates when a hacker makes use of a web application to deliver/plant malicious code [25] which can be in the form of VBScript, Javascript, ActiveX, HTML or Flash into a vulnerable page where the scripts in the above form are executed on the machine. Through XSS, a hacker will be able to steal personal information, steal cookies; user's identity can be spoofed [26]. Unknowingly, users execute these scripts while they are browsing/views dynamically generated pages/documents of the matter provided by the attacker [27].

3.2.2.1 Typical XSS attack

Referring to the Figure 5 below, the user (victim) is fooled on clicking a link by many different ways by the attacker. It can be just a normal link in a HTML based e-mail, a banner or also it can be a flash script which is embedded in a web page. The victim does not know that there is an embedded script behind the click of such actions. When the victim clicks on such links, the web server returns the page with the embedded malicious script attached to it thus executes it without the victim's knowledge.

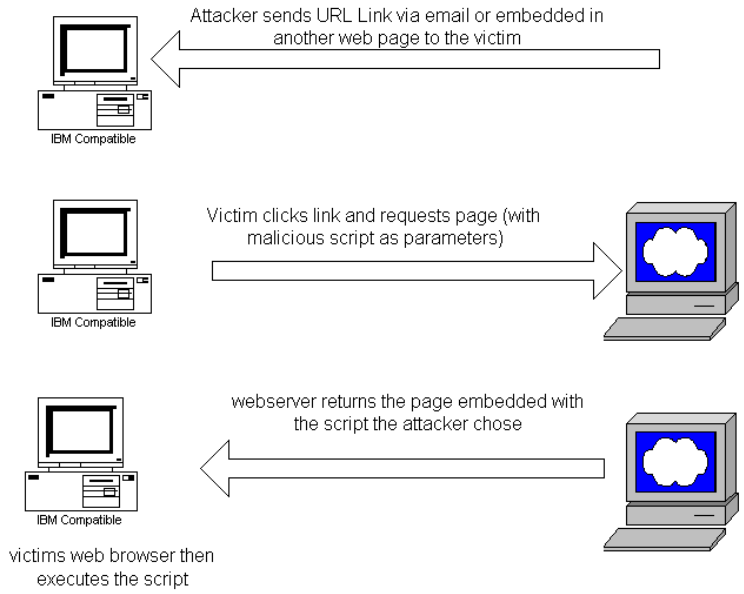

Fig. 5. XSS attack
Courtesy of www.cgisecurity.com[28]

3.2.2.2 Control measure to prevent XSS attack

- Filter the data: Filter the internal and external inputs which will identify and remove keywords such as <script> tag, Javascripts commands, CSS styles and various other HTML markups [29].
- Escaping: Applying escaping will direct the client browser informing that the data which is getting passed through shouldn't be deciphered in other means. Within HTML, escaping is done by applying &# followed by its respective character's code. Escaping is applied to Javascript, CSS and also to the data which is in the XML format. ESAPI by OWASP and AntiXSS by Microsoft are two of the most popular escaping libraries available for the developers [29].

3.3 Insider Attacks

As the economy keeps on changing, companies needs to adapt strategies to expand and reduce their workforce as per the business needs. Such amendments will affect the roles and responsibilities assigned to the concerned employee's role. Processes are not followed when it comes to restrict a particular system or access to an employee as he/she may not be fitting for that role. Once a person has been promoted from technical to operations still their access to the technical systems are alive and not discontinued. This flaw in the system leads to an increase in the systems exposure to an unauthorized employee which in turn results in Data corruption, deletion/modification, sensitive data leakage, stealing corporate data etc.

3.3.1 How you become a victim of Insider Attacks?

An insider is an employee of the company who has established trust with the organization and has been granted access to the resources/assets based on authentication followed by authorization [30].

An employee has left the manager's room in a distress as bonus has been denied. Being disgruntled the employee takes a look around and watches other colleagues working. Taking advantage of this situation of no one looking, the employee starts working on the computer and logs on the company's financial systems. The employee amends few records within the database which in turn results in the change of his own record giving him the bonus himself.

3.3.1.1 Control measures to prevent Insider Attacks

- **Identify and protect organization's assets:** Organization should be able to identify its assets (money, data, systems etc.) and also what measures have been taken to safeguard/protect them. E.g.: To protect the company's data, the management should know what kind of data it is (either physical or electronic), where has the data stored (server or physical file shelf), the method to access the data (physically or over the network), which all departments have access to it (Managers/Employees/Consultants etc.), if any changes are made to the concerned data , how are those changes getting logged and finally what mechanism is taken to protect the data (username & passwords / lock & key). Once the above factors are in place, the management should decide who, among the employees, will have access to such assets. Once validated, the access has to be removed for the rest of the employees irrespective of their position hierarchy [30].
- **File Sharing over the network:** It is very common to see that colleagues of the same team often share project documents over the network by creating a shared common folder without thinking that who else will be able to access the very same information outside the team. E.g.: If the finance team of an organization creates a folder which has all the banking details of the employees and has share the very same folder for his/her colleagues to extract the information without setting any access rights/permission. It is very dangerous to share everything internally thinking the employees are very good, but you never know who might turn out to be an inside attacker if such information is accessible.
- **Detect Physical Access:** As employees are allowed in the company's premises/other colleagues work stations, internal physical system which detects the presence of employee should be in place. Physical System comprises of many things which includes a camera system which can be placed where the company's critical servers are kept. Also it can include a card swipe mechanism which helps the management to track the incoming/outgoing of the employees within the critical areas in the organization.
- **Limited Access to Database:** Organization's database consists of very sensitive information such as the employee's payroll/personal details, clients list etc. Database systems are the primary target for insider attacks. To protect from such incidents, administrators should restrict the percentage of access to the database granted to the users. Only privileged users should have the Read/Write/Update access to the information. All the actions performed over the database needs to get logged [32].
- **Conduct regular trainings :** Employees should be given training / educational session to follow very basic security practice such as locking/logging out their PCs while they are away from their workstations, never to share their password with anyone or never to write down their passwords anyplace which is accessible. Also they should be trained to not to have passwords which can be very easily predicted [32].
- **Have a formal hiring process:** Never hire a person just because you have been referred to him/her by your friend. Professionalize your hiring by doing background/criminal checks [33].

3.4 Wireless network breaches

Today is the era of wireless computing. Most of the organizations have their own implementation of wireless network. But are they secured and encrypted? Hackers/attackers are looking for such wireless networks to hijack them and carry out their attacks through the very same breached network. SMEs tend to ignore to safeguard their wireless networks not thinking about the consequences.

3.4.1 Consequences of not securing/protecting the wireless network?

- **Privacy breach:** When an Internet is be-

ing used for surfing, packets are being send from one point to another point. These packets can be captured by the hacker and manipulate them by penetrating into them. By doing this, the hacker will have straight access to the usernames, passwords, customer's data, financial information etc [34].

- **Slowness in surfing:** If outside users who are not part of your network are using your wireless network for their personal activities like uploading & downloading various contents, the users of the organization will experience very slow speed which may cause delay in delivering their tasks where they have to refer to the Internet to gain information [34].
- **Unlawful traffic generation:** Outside users are carrying out illegal activity via the organization's wireless network. This may result in legal affairs for the organization which may hamper their brand, user's trust, lead the company's profits to a downfall etc [34].
- **Exceeding Data Usage:** Certain organizations have agreements signed with the Internet Service Providers (ISP) in limiting the data usage. If unwanted outside users are accessing your network and using it for their personal/malicious tasks, this might lead the organization's account to be violated in their terms and conditions with the ISP [34].

3.4.2 Control measures to prevent wireless network attack

- **Amend the default password:** The concerned person within the organization should amend the default router's password once the wireless network has been set up. Hacker's are normally able to guess the default passwords which simplifies their launch of attack [36].
- **Encrypt the network:** Encryption is one of the most essential security measures to be implemented to secure an organization's wireless network. Encryption can be achieved by WPA2 encryption which gives good security mechanism than the previous WPA and WEP technologies. Within WPA2, organizations should choose the most appropriate for their network [35].
- **Enabling MAC Filtering:** Limit the wireless network users to only specific MAC Address by enabling the feature of MAC filtering [35].
- **Set DHCP Limit:** DHCP manages very easily for the network to restrict the no. of devices that can be connected to the wireless network [35].
- **WAN Requests to be blocked:** This option should be enabled as to hide the network from other Internet users. Enabling this option will make the router to not to respond to the incoming IP requests from the external remote users restricting them from hijacking information from the network [35].
- **Change the SSID broadcast:** Change the default SSID name to a much stronger name. A stronger name discourages the hackers from targeting the network [35].

3.5 Wi-Fi Hotspots

You are sending a confidential e-mail to your Manager by connecting to the Internet via the free Wi-Fi hotspot next to your the coffee place which you normally visit. The very same is being accessed by the person sitting right opposite to your table. One of the hacker's prime weapons to carry out their attack is through free public Wi-Fi hotspots. Wi-Fi Hotspots which are publicly available are normally unsecured. Connectivity over free Wi-Fi networks means you are sharing the same network with different people. You should not connect your organization's information without protection. Hackers/Attackers normally set up an unsecured access point who SSID will be broadcasting as Free Wi-Fi or any similar text. They wait for victims to fall prey for such SSID. Having Packet Sniffers installed on their machines, hackers are able to sniff the packets and are able to see everything the user is performing on his/her PC. They are able to capture the packets where the employee types, including login details, session id etc. in real time [33].

3.5.1 Control measures to protect from Wi-Fi Hotspots attacks

- **Choose Encrypted Connection –** When using the organization's computer to connect to the network via a public available free Wi-Fi, make sure to connect via Virtual Private Network (VPN). The advantage of such is that it will encrypt the data stream, so even if the hacker is capturing the incoming-outgoing packets from your machine, it will be very vague/unintelligent for them to decipher the content of it. Always select an encrypted connection while connecting to a Wi-Fi. Such networks will require a password and it will show the type of encryption being used [33].
- **Choose highly known hotspots –** Never choose a hotspot just because it is available free from an unknown venue. Always select from a reputed area/place/venue as they have been set up keeping user's safety keeping their user's trust/business reputation as a priority. Organization's staff should be trained on selecting such hotspots [33].
- **Safeguard your sensitive data –** Hide folders that contain sensitive data in the machine while connecting to such hotspots. This is one way to harden the search for the attackers to upfront find the sensitive data residing in the hard drive [36].
- **Never save passwords –** Various websites and browsers frequently asks to save the passwords. Never store passwords on such requests while browsing the internet via the hotspot [36].
- **Surf via HTTPS and SSL –** Websites uses HTTPS and SSL to connect to them making the connection secured and encrypted. While connecting to a hotspot, make sure to surf such websites by such protocols [36].
- **Implement Windows Firewall –** Enable the windows firewall which connecting to any public Wi-Fi hotspots. Choose the settings for public network under windows firewall for secured access [36].

4 Conclusion and Future work

To sustain within the economy and to increase their profits in their business, SMES are depending on Technology/Internet on a much broader scale. Fast growth of the Internet has increased threats/attacks where most of the SMEs are at disadvantage in order to safeguard their business/products against the attacks conducted by the hackers. Big organizations (sectors such as finance, telecom, retail, IT) depend on SMES by outsourcing their services to them and have to make sure SMES follow an equal protection mechanism from cyber threats. Over the past few years the demand for the services which SMES offer has highly increased.

In this paper, we have identified few of the major cyber security threats along with their counter measure within SMEs. IT Security expertise, financial budgets are few of the constraints where SMEs do not want to invest in the protection mechanism. This paper provides understanding of such attacks and how to mitigate them at a minimal cost. Once threats are well understood by the organization and the right protection is implemented, they will be able to achieve their targeted results without any disruption in their services. Our future work will include bringing out various other cyber security threats such as Unauthorized Internet Surfing, E-mail attacks, Social Engineering, Usage of Unauthorized devices etc. which are still persisting within a SME and how they can protect themselves from such attacks.

References

[1] D.Spinellis, S.Kokolakis and S.Gritzalis, "Security requirements, risks and recommendations for small enterprise and home-office environments," *Information Management & Computer Security*, 1999, pp.121-128.

[2] A.Tawileh, J.Hilton and S.McIntosh, "Managing Information Security in Small and Medium Sized Enterprises: A Holistic Approach," School of Computer Science, Cardiff University.Available:http://www.tawileh.net/anas

//files/downloads/papers/InfoSec-SME-ISSE.pdf?download

[3] Microsoft Small Business Team, "Security Guide for Small Business" Available: http://www.microsoft.com/smallbusiness

[4] **GFI**, "Security Threats: A Guide for small and medium businesses" Available: www.gfi.com/whitepapers/Security_threats_SMEs.pdf

[5] U. Vijayakumar (2009). Top Management Control Functions for Information Systems in Small and Medium Enterprises. *Informatica Economică Journal* [Online]. Available: http://www.revistaie.ase.ro/content/52/11-%20Vijayakumar.pdf

[6] C.Onwubiko and A.P.Lenaghan, "Managing Security Threats and Vulnerabilities for Small to Medium Enterprises" in Proc. *IEEE International Conference on Intelligence and Security Informatics 2007*.Available: http://www.research-series.com/cyril/IEEE-ISI07.pdf

[7] Information Systems Security Association, UK, ISSA-UK 5173, "Information Security for Small and Medium Sized Enterprises," March 2011, Available:http://www.issa-uk.org/issa_5173/ISSA-UK_Draft_Standard_on_Information_Security_for_SMEs.pdf

[8] J.Park, R.J.Robles, C.Hong, S.Yeo and T.Kim, "IT Security Strategies for SME's,"*International Journal of Software Engineering and its Applications, and its Applications,* Vol.2, No.3, July, 2008, pp.91-98

[9] R.Kissel, "Small Business Information Security: The Fundamentals," *National Institute of Standards and Technology NISTIR 7621*, Available: http://csrc.nist.gov/publications/nistir/ir7621/nistir-7621.pdf

[10] P.Alexander, "Is your Biz Safe From Internet Security Threats?" July 11, 2005, Available: http://www.entrepreneur.com/article/78616

[11] CBCNews, "New computer virus a throwback" September 10, 2010, Available: http://www.cbc.ca/news/story/2010/09/10/con-computer-virus.html

[12] R. Morgan, "Information Security for Small Businesses," Available: http://www.infosecwriters.com/text_resources/pdf/Information_Security_for_Small_Businesses.pdf

[13] IT Business Edge, "Top 10 Cyber Security Threats of 2011 and Beyond," Available: http://www.itbusinessedge.com/slideshows/show.aspx?c=87289

[14] Cisco Systems, "Top Five Security Issues for Small and Medium – Sized Business-es,"Available:http://www.cisco.com/global/EMEA/sitewide_assets/pdfs/you_inc/Top_Five_Security_Issues_for_SMBs.pdf

[15] Microsoft Safety & Security Center, "How to recognize phishing email messages, links, or phone calls," Available: http://www.microsoft.com/security/online-privacy/phishing-symptoms.aspx

[16] T.V.Srivastava, "Phishing and Pharming – The Deadly Duo," *Sans Institute*, January 29, 2007, Available: http://www.sans.org/reading_room/whitepapers/privacy/phishing-pharming-evil-twins_1731

[17] A.Elledge, "Phishing: An Analysis of a Growing Problem," *Sans Institute*, January 2007, Available: http://www.sans.org/reading_room/whitepapers/threats/phishing-analysis-growing-problem_1417

[18] Microsoft Safety & Security Center, "Protect yourself from cybersquatting and fake web addresses," Available: http://www.microsoft.com/security/online-privacy/cybersquatting.aspx

[19] S.Northcutt, "Spear Phishing," *Sans Institute*, May 9, 2007, Available: http://www.sans.edu/research/security-laboratory/article/spear-phish

[20] Microsoft Safety & Security Center, "Email and web scams: How to help pro-

tect yourself", Available: http://www.microsoft.com/security/online-privacy/phishing-scams.aspx#Tools

[21] E.R.Storoie and A.C.Rusu (2011), Security Risk Management – Approaches and Methodology. *Informatica Economică Journal* [Online]. Available: http://revistaie.ase.ro/content/57/21%20-%20Stroie,%20Rusu.pdf

[22] Wikipedia, "Web application security," Avaiable:http://en.wikipedia.org/wiki/Web_application_security

[23] J.D.Meier, A.Mackman, B.Wastell, P.Bansode and A.Wigley, "How To: Protect From SQL Injection in ASP.NET," *Microsoft patterns & practices*, May 2005, Available: http://msdn.microsoft.com/en-us/library/ff648339.aspx

[24] J.Weinberger, P.Saxena, D.Akhawe, M.Finifter, R.Shin and D.Song, "A Systematic Analysis of XSS Sanitization in Web Application Frameworks," *ESORICS 2011,LNCS 6870*, pp.150-171, 2011. Available: http://www.cs.berkeley.edu/~dawnsong/papers/2011%20systematic%20analysis%20xss

[25] The Open Web Application Security Project, "Cross-site Scripting (XSS),"Aug'2011, Available: https://www.owasp.org/index.php/Cross-site_Scripting_(XSS)

[26] Acunetix, "Cross Site Scripting Attack," Available: http://www.acunetix.com/websitesecurity/cross-site-scripting.htm

[27] P.Lee, "Cross-site scripting," *IBM*, Sep'2002, Available: http://www.ibm.com/developerworks/tivoli/library/s-csscript/

[28] CGI Security, "Attacks on the Users Cross-Site Scripting," Available: http://www.cgisecurity.com/owasp/html/ch11s02.html

[29] J.Pullicino,"Preventing XSS Attacks," *Acunetix*,Mar'2011 Available: http://www.acunetix.com/blog/web-security-zone/articles/preventing-xss-attacks/

[30] B.Ruppert, "Protecting Against Insider Attacks," *Sans Institute*, Apr'2009, Available: http://www.sans.org/reading_room/whitepapers/incident/protecting-insider-attacks_33168

[31] N.Einwechter, "Preventing and Detecting Inside Attacks Using IDS", *Symantec, Nov'2010, Available*: http://www.symantec.com/connect/articles/preventing-and-detecting-insider-attacks-using-ids

[32] N.Einwechter, "The Enemy Inside the Gates: Preventing and Detecting Inside Attacks,"*Symantec*, Nov'2012, Available: http://www.symantec.com/connect/articles/enemy-inside-gates-preventing-and-detecting-insider-attacks

[33] S.Pinzon, "Top 10 Threats to SME Data Security,"*WatchGuard*, Oct'2008, Available: http://www.watchguard.com/tips-resources/whitepapers/top-10-threats-to-sme-data-security.asp

[34] HP, "Protecting your wireless network," Available: http://www.hp.com/sbso/wireless/ipg/mobileprint/security.html

[35] A.Wawro, "How To Lock Down Your Wireless Network," *PCWorld, Nov'2011, Available*: http://www.pcworld.com/article/243290/how_to_lock_down_your_wireless_network.html

[36] S.Lynn, "Ten Tips for Public Wi-Fi Hotspot Security,"*PCMag.com*, Sep'2012, Available: http://www.pcmag.com/article2/0,2817,2368802,00.asp

Nilay K SANGANI completed his B.Tech in Computer Science & Engineering from National Institute of Technology, Calicut, India in 2008.Presently; he is working with Emirates Group IT as a Software Engineer. Simultaneously, he is pursuing his M.E. in Software System from BITS, Pilani-Dubai Campus. His area of interest includes IT Security, Web Application Security, Secure Software Development, Data Mining and Pattern Analysis.

Balakrishnan VIJAYAKUMAR holds a PhD in Computer Science from BITS, Pilani, India in 2001. He has 20 years of university teaching experience in CSE (National Institute of Technology, Tiruchirappalli, India and BITS, Pilani-Dubai Campus, UAE) and 6 years of experience in computer industry. Presently, he is working as Associate Professor, CS, BITS, Pilani-Dubai. His areas of interest include Distributed Database Systems, Component Based Software Engineering, Web Mining, Multimedia Systems and Open Source Software Development. He is member of professional bodies ISTE (Indian Society for Technical Education), World Enformatica Society and Staff Advisor for Linux Users Group, BITS, Pilani-Dubai Campus. He is actively involved in organizing and judging committee member in annual students' technical event TECHNOFEST at BITS, Pilani-Dubai Campus. He has been involved in co-ordination and coaching for the students of BITS, Pilani-Dubai Campus, for annual UAE National Programming Contest since 2005.