UNIVERSITY OF TWENTE.

The Impact of Cyber Security on SMEs

Nabila Amrin

Faculty of Electrical Engineering, Mathematics and Computer Science

Graduation Committee: Prof. Dr. Pieter Hartel
Prof. Dr. Manrianne Junger
Arthur Leijtens

Abstract

Cybercrime in the Small Medium Enterprises (SMEs) environment is a growing concern. SME's dependency on Information Technologies and Internet has opened the door to vulnerabilities to cybercrime. These vulnerabilities are making information security a critical issue for all SMEs. Unfortunately, cybercrime prevention is often neglected within the SME environment. This study aims to be a pilot research for conducting an empirical study by surveying SMEs in Europe on their security practices and position toward current technological trends like Cloud Computing and Bring Your Own Device (BYOD). To achieve the aim of the study a questionnaire has been produced. Sixteen SMEs from different business operations, registered in Europe, were interviewed on their recent IT security trends, cybercrime victimization, and cybercrime prevention practices. The main findings indicate that the level of IT security of the respondent SMEs is not to a decent point. The implementation of written security policy is present in the SME environment, but it is not very common. In addition, European SMEs fall behind than Australian organizations in order to implementing IT security measures and policy. BYOD and Cloud Computing are accepted technological trends among respondents. However, the result of the study shows that SMEs are not cognizant of the vulnerabilities related to BYOD and Cloud Computing. 4 out of 16 respondent SMEs reported cybercrime victimization incidents over the period 2013-2014. SMEs are simply unaware of IT-related security incidents, because victimized SME does not spread the news fearing further reputational damage. Referable to the smaller sample size, the results are inconclusive to prove any fact related to cybercrime practices. Further research spanning a longer period of observation must be done in order to obtain responses from more SMEs. The questionnaire developed for this study is tested and it can used as a questionnaire for a larger study.

Contents

List of Tables

List of Figure

1. INTRODUCTION

There is a significant rise of the Internet as a medium of business operation for Small Medium Enterprises (SMEs), and it has exposed SMEs to the threats of Cybercrime. Over time, Information Technology (IT) has offered a range of opportunities to SMEs as the global means of communication and business operation. However, the dependency of SMEs on IT has also made them vulnerable to newer IT security threats. SMEs can be one of the popular targets of cybercriminals for their affiliation with bigger companies as their clients. Hence, protecting SMEs from cybercrime and cyber security risks should be a major concern for SMEs themselves [1].

Over time, the numbers of cybercrime victims are increasing, making it a growing global concern. According to the Federal Bureau of Investigation (FBI) and the National White Collar Crime Center (NW3C) [2] the number of valid cybercrime complaints received in 2012 was 24,000 per month; and the amount of losses related to cybercrime increased by 8.3% since 2011. A survey conducted on 234 organizations from different countries stated that, the organizations have experienced 20 percent more successful cyber-attack in 2013 than the previous year [9].

With the increasing number of cybercrime victims, its associated cost is likewise increasing. The FBI report [2] states that the costs related to the cybercrime victimization is about $525,441,110. Another report by HP enterprise [33] found that the average cost of cybercrime in the UK is 2.99 million pounds per year. The report [33] sampled 36 organizations from the UK. The Norton Cybercrime Report [3] states that the total global direct cost of cybercrime has increased to US$113 billion in 2013. However, according to

McAfee Inc. worldwide the actual annual cost is almost 10 times more than the amount described in the Norton Cybercrime Report [3], approximately $1 trillion [4]. Reports related to cybercrime costs are based on different types of samples; hence, the cost estimate is unreliable [5]. For example, the FBI report [2] is based on formal report to FBI about financial loss for the US citizens in one year. The Norton Cybercrime Report [3] sampled online adults all over the world to measure cybercrime and the reported cybercrime cost is not guaranteed as formal or reported to any authority like FBI report, which is the same way sampling McAfee Inc.'s report [4]. Both of the gathered information about cybercrime. In addition, the samples in The Norton Cybercrime Report [3] and McAfee Inc.'s report [4] are both gathered from anonymous online adults and thus questions the credibility in stating total high global cost (more than 100 billion dollars) of cybercrime. According to Kaspersky's Global Corporate IT Security Risks Report 2013 [6], a serious incident can cost a large company on average of $649,000; for small and medium-sized companies the cost is close to $50,000 on average. A successful targeted attack on a large company can cost it $2.4 million in direct financial losses and additional costs. For an SME, a targeted attack can cost about $92,000 on average, which is almost twice as much as an average cost ($50,000 on average as mentioned before). This amount of loss can be substantial for an SME to continue its business.

1.1 RESEARCH SCOPE

The increase of IT and Internet in SME business operation has introduced cybercrime to their business operations. It is nevertheless hard to obtain an accurate report on security threats in any organization for the fast adoption of engineering. The list of top 10 most common [10] threats for security vulnerability gives an overview about what kind of weaknesses an organization can suffer due to the espousal of new technological trends.

The technological trend indicates what are the most used technologies in a business environment are in the current time. Business organizations are constantly looking for the lower cost of IT and thus adopting trends that guarantee the lowest IT cost. Aligning business with the technological trends allows the them to use the most updated technology adopter. Some of the technological trends are the use of Cloud Computing, BYOD, big data analytics and the usage of social media. The security threats of two technological trends named Cloud Computing and BYOD will be discussed in the later part of the study.

Nevertheless, it is necessary to receive a fuller apprehension of the concept of IT and cyber security of SMEs. A literature study aims to answer the following questions:

1. *What are the IT security threats of SMEs?*
2. *How do Cloud Computing and BYOD influence IT security threats?*
3. *What are the IT security scenarios of SMEs in Europe?*

The structure of the paper is as follows. Section 2 contains the literature study, which takes a closer look into IT security threats in details. The section 2 is divided into segments of the method of the literature study, describing key words of SME, the relationship with SME and IT security, ten security threats on SMEs and its prevention, brief discussion on definition and prevention of Cloud Computing and BYOD and discussion about paper related to cybercrime done by commercial and peer researchers. Section 2 is concluded with a discussion on the research questions and the expectations of the survey result. Section 3 is divided into the methodology for the research and a brief discussion of the questionnaire. Section 4 describes the result of the study. Section 5 and 6 outlines the limitation and conclusion respectively.

2. LITERATURE STUDY

2.1 AIM OF LITERATURE STUDY

The primary goal of the literature survey is to gain background knowledge of the IT security threats on SMEs. This section also tries to find out various concepts relating to IT security threats and its potential prevention. The literature study also attempts to identify possible areas for further research on IT security threats. Therefore, the threats of cloud computing and Bring Your Own Device (BYOD) will be discussed in details. As well, the literature study section defines key terms, definitions and terminology related to this research. In the end the literature study investigates respective peer and grey literatures on cybercrime. In addition, the aim of the literature study is to get some support for the design of research methodology.

2.2 METHOD OF LITERATURE STUDY

During the period of February 2014 until April 2014, online databases were searched for information on cybersecurity. The database used for keyword searching were Scopus and Google Scholar. As mentioned before, the objective of the research is to investigate SME IT security scenarios. First, the search key words were “SME IT Security”, “Small Medium Enterprises IT security” and “Small Medium Business IT security”, which returned total 573 hits. Second, by refining out the results to more appropriate and meaningful to the research, keywords like “Security”, “Survey”, “Culture”, “Risk”, “Assessment” and “Policy” have been used as “AND” operator with the three main research keywords mentioned above. These resulted 122 hits. After going through the abstracts and conclusions, these 122 papers were reduced to 10 research papers focusing

on IT security and trend of SMEs. Third, few of the articles/papers were obtained from "similar studies" on Scopus for the mentioned keywords.

Fourth, after studying researches on IT security threats, the present study wanted to focus on two specific security threats, namely Cloud Computing and BYOD, which interested the researcher most. Therefore, the key words "BYOD", "SME Cloud Computing" were used to find research papers. However, "BYOD" and "SME Cloud Computing" mostly incurred reviews from different articles in scientific magazines. The keyword "Cloud Computing" incurred an enormous number of IEEE papers of that technology, but the studies were only limited to effects of Cloud Computing on the organizations. Fifth, the commercial/grey studies, keywords like "IT Security Survey" AND "2012/2013" were used. The queries used for this study are mentioned in Table 1. As presented in the Table 1, ((TITLE-ABS-KEY(SME IT Security) returns the documents as TITLE-ABS-KEY(SME AND IT AND Security). By default the Scopus search use AND operation for any two given words.

Table 1: Keywords searched for the research

Keywords searched for peer review		
((TITLE-ABS-KEY(sme it security)	Scopus	91
((TITLE-ABS-KEY(small medium enterprises it security)	Scopus	186
((TITLE-ABS-KEY(small medium business it security)	Scopus	296
Total		**573**
Below mentioned keywords were used as AND operation with the above 3 keywords		
TITLE-ABS-KEY((sme it security AND survey) OR (small medium enterprises it security AND survey) OR (small medium business it security AND survey))	Scopus	47
TITLE-ABS-KEY((sme it security AND culture) OR (small medium enterprises it	Scopus	19

security AND culture) OR (small medium business it security AND culture))		
TITLE-ABS-KEY((sme it security AND risk) OR (small medium enterprises it security AND risk) OR (small medium business it security AND risk))	Scopus	56
Total		**122**
BYOD SME	Google Scholar	64
Cloud Computing AND SME	Google Scholar	59
Key words used to select paper by reading abstract		
Survey, Security awareness, policy and risk assessment		10
Keywords searched for Grey studies		
IT Security Survey And 2012/2013	Google	Over 20

The remaining of the literature study is structured as follows. In section 2.3, the study will briefly describe the definitions of SMEs and different scenarios of SME environment. Section 2.4 will discuss the relation of SME and IT security and important terminologies of IT security. Section 2.5 contains a description of the most common security threats oriented to SMEs and its prevention. Section 2.6 and 2.7 will focus on the impact of security threats related to Cloud Computing and BYOD, their definitions, their current impacts on SME, threats and prevention. Section 2.8 will discuss studies related to cybercrime and various surveys done by both commercial organization and perspective peer researchers. The literature study will be concluded with a discussion and related expectation for the result of this study.

2.3 SME

There is no single definition of SMEs (Small Medium Enterprises). The European Commission has developed criteria for being an SME based on its employee numbers, turnover and balance sheet statistics [44]. According to the European commission, the category of micro, small and medium-sized enterprises (SMEs) are made up of

enterprises that employ fewer than 250 persons, which have an annual turnover not exceeding 50 million euro, and/or an annual balance sheet total not exceeding 43 million euro [45]. The SME can be categorized among themselves as medium, small or micro SMEs based on their employee numbers, turnover and balance sheet are described in Table 2 below.

Table 2: SME categories based on employees, turnover and balance sheet

Company category	Employees	Turnover	Balance sheet total
Medium-sized	< 250	≤ € 50 m	≤ € 43 m
Small	< 50	≤ € 10 m	≤ € 10 m
Micro	< 10	≤ € 2 m	≤ € 2 m

Although SMEs is comparable in size, turnover and balance sheet, they can differ in their regular business operation. Below some scenarios can give a vivid picture of different categories of SMEs. These scenarios are based on how the number of employees and the product SME sells make a difference in its IT operation.

***Scenario 1*:** A small home based SME selling homemade jewelry, where the number of employees can be one or two. They can reach their clients via a website. In this kind of SME, low capital and low IT budget are expected.

Scenario 2: A garage for car with 20 employees. They repair cars and can manage all the transaction/payment to customers via a website. As well, there is no employee with an IT background. They hire external IT Company to take care of their IT.

***Scenario 3*:** An SME with 70 employees selling software solution to other companies. They have their own IT department. They have a big budget for IT infrastructure and have employees designated for IT security matter.

2.4 SME AND IT SECURITY

For defining protection measure of IT, first we have to determine what can be affected by IT security threats. Terms like asset, threat, and vulnerability are often used in IT security studies to describe further IT security concepts. Table 3 describes those security terms for better understanding.

Table 3: Description of Asset, Vulnerability and Threat

Key Words	Description
Asset	According to ISO 27005 [11], an asset is anything that has importance/value to the organization. The assets can be of different types. It can be infrastructure like buildings, computer equipment, software code, development tools, information like database information, IP (Intellectual Property). Even reputation can be recognized as 'valuable' asset to the organization [12].
Vulnerability	Vulnerability is defined as a weakness in an asset that gives the chance to be exploited and harmed by threats [13]. According to Open Group's risk taxonomy [14], vulnerability defines the probability of an asset's inability of defending an attack agent. Vulnerability occurs when there is not enough resistance against the threat agent.
Threat	A threat can be a potential cause that can be turned into an unwanted incident to damage an organization [13].

2.5 IT SECURITY THREATS OF SMES

According to US State of Cybercrime Survey [8], SMEs are unknowingly increasing their cyber-attack threats that increases vulnerabilities by adopting various means of IT. The most common IT vulnerability trends right now are social collaboration, expanding the use of mobile devices, moving the storage of information to the cloud, digitizing sensitive information, moving to smart grid technologies, and embracing workforce mobility alternatives. Watchguard.com [10] has presented a list of IT security threats that is most harmful to SMEs of US in their opinion. "WatchGuard" provides expert guidance and support to its huge number of customers who are mostly SMEs. WatchGuard monitors emerging network security threats daily, with a special focus on issues that affect SMEs. WatchGuard's approach produces a practical report on IT security threat by constantly refining input related to negative affect of security threats from their clients. This is how WatchGuard claims to form carefully considered conclusions on what types of data compromises most often occur in the real world SMEs. In addition, there are not many papers (white paper or scientific) focusing on listing SMEs IT security threats in particular. There is "The Verizon Data Breach Report 2014" [31] which analyzed more than 1,300 confirmed data breaches and pointed out similar security threats (Insider misuse, web app attacks etc.) as the "WatchGuard" paper [10]. However, the Verizon Report's data breach report is not based on only SME's cyber security threat as the report is based on data gathered from 50 national or international cybersecurity organizations and the samples are limited and not random. Many cybercrime reports like [33] discusses the frequency of occurrence of cybercrime and the financial loss associated with it. Most of the reports [33] address the incident, but not the cause of the incident. In addition, WatchGuard" paper [10] describes the necessary preventive measures related to these threats. Although the preventive measures described in the WatchGuard paper [10] include commercial solution and software provided by them. The mentioned security

threats in WatchGuard" paper [10] are also investigated from different sources/papers to present the complete pictures of the threats and how it affects SMEs IT assets. In addition, the preventive measures described in this study are widely investigated and does not include commercial solution of WatchGuard" paper [10]. The discussion of each of the security threat consists of its definition, the IT asset it compromises and the corresponding prevention an SME can adopt. The security threats are discussed below.

2.5.1 AUTOMATED EXPLOIT OF A KNOWN VULNERABILITY

These are non-targeted attacks because these attacks attempt to compromise computer's operating system having any known security vulnerability. Most of the automated attacks try to exploit vulnerabilities in Windows. These attacks occur if all necessary patches are not installed. SMEs sometimes neglect installing the latest patch due to the low number of technical staff or for simple ignorance [10].

Main Asset that gets compromised: The Operating System (OS) of the computer.

Prevention: The SME can use patch management software to scan network, identify missing patches and software updates, and distribute patches from a central console to have the entire network up to date. Also, SMEs can train the employees to comply with the up to date patches by themselves [10].

2.5.2 *MALICIOUS HTML EMAIL*

This type of email attack arrives as an HTML email that links to a malicious, booby-trapped site. When the user mistakenly clicks on any link on that malicious website, the click triggers the automatic download of an exploit from that website [10].

Main Asset that gets compromised: Computer, mobile phone, tablet any equipment that can view the malicious emails.

Prevention: The SME can implement aggressive spam filtering so this kind of emails does not appear in the user's inbox. It is also necessary to raise employee awareness about email security. Employees must be made aware of spam emails. An SME can implement periodic training for employees about recognizing spam email [10].

2.5.3 RECKLESS WEB SURFING BY EMPLOYEES

Employees can surf non-business-related sites using the company's electronic devices. This reckless web surfing can affect company network with bot clients, Trojans, spyware, and different kinds of malware [10]. The sites that spread the most malware are 1. Celebrity fan sites, 2. Casual gaming sites and 3. Porn sites [65]. As well, online social networks are being targeted by malware [66] and employees surfing online social network using company computers may put the whole company network under malware attack.

Main Asset that gets compromised: Computers, tablets, mobile phones connected to the company network.

Prevention: The employees should be advised not to surf any website other than work related sites. Also the employees should be acknowledged that all the internet surfing log is monitored so they do not surf unethical websites during work. Implementing policy related to "Acceptable Use Policy" of the Internet is necessary. Finally, web filtering solutions can block those non-work related URLs, to enforce the "Acceptable Use Policy" of internet on the employees [10].

2.5.4 WEB SERVER COMPROMISE

One of the common botnet attacks is against the website. Most of the SMEs have a website to communicate with their customers. The website can be vulnerable if it has poorly written custom code, leaving a lot of security holes to be exploited by attackers. Attackers can compromise the company website, and make it a slave server to unwillingly spread malware [10].

Main Asset that gets compromised: Company's website and server.

Prevention: The best way to prevent this attack is to audit the web application code and fix all the security holes that can be exploited. Also, using a firewall that can filter malicious traffic to the server will be helpful to prevent web server compromise attack [10].

2.5.5 DATA LOST ON A PORTABLE DEVICE

This type of vulnerability occurs due to stolen portable electronic device. Sensitive data can be stored in a portable device like a laptop, mobile phone or tablet. And if these devices get lost or stolen, the sensitive data can be compromised. Portable devices like laptops or mobile phones are always at a high risk of being stolen. For instance, it is estimated that over 8 million cell phones are lost or stolen each year [32]; often the loss of a cell phone means the loss of personal data and massive aggravation. This alarmingly high number of stolen devices indicates the severity of the data loss problem due to stolen device.

Main Asset that gets compromised: Portable device and the sensitive data stored in it.

Prevention: Most mobile devices have the option of encrypting all user data on the devices, and/or requiring a password to access the data. There should be a policy requiring all employees to use that particular feature for the portable devices used for

work. Use of Mobile Device Management (MDM) software that helps the company to manage mobile devices and wipe all data on the device in case of necessity [10].

2.5.6 RECKLESS USE OF WI-FI HOTSPOTS

Attackers can set up a Wi-Fi access point and leave the access point free or open to attract victims. If the victim accesses the internet using that Wi-Fi access point, the attacker can monitor all the traffic of the victims and steal valuable information such as login credentials to important website from the monitored data [10].

Main Asset that gets compromised: Company related sensitive data.

Prevention: The employees should be advised to always choose encrypted connections. Also, they should be asked to not connect portable device to unknown Wi-Fi connection.

2.5.7 RECKLESS USE OF HOTEL NETWORKS AND KIOSKS

Hotel networks most of the time provide free Wi-Fi that can infect devices with worms, viruses, spyware and malware. Laptops that do not have up-to-date personal firewall software, anti-virus, and anti-spyware can get compromised by connecting to this type of Wi-Fi connection. Later, when the employee attaches his/her devices to the company network, it can infect the whole company network [10].

Main Asset that gets compromised: Company's entire network and employee's device.

Prevention: Devices like laptops, smartphone, tablets should have the updated antivirus, anti- spyware/malware, and firewall. Also policy should be implemented that employees can never turn off security defenses of the devices [10].

2.5.8 POOR CONFIGURATION LEADING TO COMPROMISE

The security configuration of any computing system is set to its default from the beginning. The users have to change the default setting to something secretive. If users have poor understanding of computing system, some settings stay default. The default credential of any system can be found on the Internet and by using that credential, attacker can log into network resource. Verizon's Business report stated that, on the causes of 500 real-world data breaches, 62% of breach caused due to poor configuration of technology [16].

Main Asset that gets compromised: Company's entire network.

Prevention: While installing network devices, always change the default username and password. Before installing a solution permanently, it is better to use the solution beforehand to check if it is easy to use by all the users, so the users will not get confused by the complicacy of the technology.

2.5.9 LACK OF CONTINGENCY PLANNING

A lot of SMEs do not have IT continuity plan. So in case of IT emergency, they do not have proper back-up and cannot recover the loss easily [10].

Main Asset that gets compromised: It can affect the entire IT infrastructure of the SME.

Prevention: Developing policy for any sort of continuity is the main solution. Although developing policy can be a hard task, an external expert can help in this case [10].

2.5.10 INSIDER ATTACKS

According to [10] insider attacks occur less frequently in SMEs than in large organizations. Because SMEs have less employees than larger organizations. As well,

illegal practices related to IT are much easier to log, notice, and correct on a smaller network of SME than in a network with a lot of employees/users [10]. One the other hand, due to a smaller employee number, SME often entrusts a lot of control of assets to a single person. This gives one employee a lot of ability to do harm as an insider. These insider attacks can range from unauthorized extraction or manipulation of data, destruction of assets, and the use of unauthorized, third-party software within the business environment (may contain harmful viruses).

Main Asset that gets compromised: The entire IT infrastructure.

Prevention: SMEs should always do basic background checks of the employees before hiring. One employee should not be given all the control of an asset [10].

From the discussion of security threats and possible prevention measures; it can be said that, most of the security threats occur from introducing new technology and the careless use of it. As most of the security threats (for example number 2,3,5,7 and 10 of the list), to some extent occur due to the employee's behavior of risk taking. Table 4 lists all the attacks that most important threats to security of SMEs in the US, according to the WatchGuard paper [10] discussed above. From the above discussion, it can also be said that, most of the security threats can be prevented by enforcing policies to control the employee's behavior. This raises the question if SMEs need to do more to protect themselves from cybercrime. The answer is simply "yes". SMEs have to put emphasis on the fact that they can get victimized by cybercriminals.

Groundbreaking new technologies are being introduced to the market almost on a daily basis that provide support and acceleration to the growth of business. Staying up-to-date with today's technology is a constant struggle in today's marketplace for organizations. It is easier to follow the general direction to which other business tends to move, also

known as “following technological trend”. IT trends indicate that the global demand for IT driven products and services used by most of the organizations. IT trend enables greater IT efficiency to business demands.

Looking at the fact that most of the SME security threats are linked to new technology and employee behavior, this study would like to investigate two technological trends that can be most crucial threats for SMEs. In this context, the upcoming trends of Cloud Computing and BYOD (Bring Your Own Device) will be discussed. The threats of cloud computing and Bring Your Own Device (BYOD) have been focused as both of these technologies/trends help SMEs to meet the reduced IT infrastructure cost.

Table 4 Top 10 Thetas to SME Data Security [10]

No.	Attack	Compromised Asset	SME's Preventive Action
1	Automated exploit of a known vulnerability	Operating System of computers	• Use patch management software • Train the employees to comply with the updated software • Implement prevention policy
2	Malicious HTML email	Devices that view email	• Implement spam filtering • Raise employee awareness • Implement prevention policy
3	Reckless web surfing by employees	Computers, laptop, etc.	• Web filtering solutions to block URLs • Use a firewall
4	Web server compromise	Website and server	• Audit the web application code to fix all the security holes • Use firewall for malicious traffic
5	Data lost on a portable device	Portable devices and data	• Encrypt data on the devices, • Use of Mobile Device Management (MDM) software
6	Reckless use of Wi-Fi hot spots	Company's data	• Use encrypted Wi-Fi connection
7	Reckless use of hotel networks and kiosks	Employee's device.	• Use updated anti-virus/spyware/malware • Use a firewall

8	Poor configuration leading to compromise	Entire network	• Change the default username and password of electronic devices • Implement prevention policy
9	Lack of contingency	Entire IT infrastructure	• Develop policy based on the company's need • Implement prevention policy
10	Insider attacks	Entire IT infrastructure	• Check the basic background of employees • One employee should not be given a lot of authority over IT asset • Implement prevention policy

2.6 CLOUD COMPUTING

The recent development of Cloud Computing has totally renovated the IT infrastructure of many companies. Instead of storing data, software, or processing power on one's own computer, Cloud Computing stores data and software on remote servers and provides customer access to them via the Internet. In addition, the end users do not own the technology they are using. The company that provides the services owns all the hardware and software. The customer organization has to pay for the service only, which is less than owning the whole IT infrastructure providing the same service.

Cloud Computing comes handy for SMEs to solve the inadequate budget for IT. Some examples of cloud service for the regular users are webmail, wiki application and Dropbox. Well-known cloud service providers are Google, Amazon and Yahoo, who have built large infrastructures to support, compute and storage in a scalable manner [54].

Advantages: This cloud model has many general benefits. A customer can modify computing capabilities, such as server time and network storage automatically without any interaction with the service provider, in *On-demand self-service*. Also the customer can use the Cloud by the internet and access through any sort of standard devices like mobile phones, laptops, and PDAs, providing the ability of *broad network access.* For the provider's side, *resource pooling* is possible where the Cloud storage and computing resource can be allocated to multiple customers on demand, with different physical and virtual resources. Cloud resource usage can be checked, measured, and reported by both the provider and customer for transparency [15].

According to Cloud Stewardship Economics Survey [26], SMEs with a relatively low annual turnover are using Cloud Computing more intensively than SMEs with a higher level of turnover. Cloud Computing offers all the functionality of current information technology services and reduces the costs of computing that used to prevent many SMEs from positioning many cutting-edge IT services. It helps the SMEs to decrease their expense and time on IT field [54].

The cost reduction of Cloud Computing can be determined by the TCO (Total Cost of Ownership). Total Cost of Ownership (TCO) in IT field, is generally used as a means to compute the total cost of owning and managing an IT infrastructure in its' useful Lifecycle [64]. In case of Cloud Computing, TCO would refer to the total cost of subscribing to the Cloud. After making TCO analysis of different types of Cloud services, Han [63] stated that, subscribing to cloud service could offer significant cost savings for organizations, rather than owning a locally managed server.

Cloud Computing as Threat: Even though Cloud Computing technology has several advantages, Cloud Computing-related risks are quite high as well. SMEs interested in securing the rewards of Cloud Computing must improve their risk management architecture [26]. The outsourcing of data to cloud introduces risks like poaching, the theft of intellectual property, proprietary software, and critical confidential data [55] [56] [57] [58].

Poaching occurs when cloud service providers abuse the user's data and resources supplied under contract. This way, cloud service providers can uncover secret plans, designs or strategies of a customer of an SME. Poaching can also lead to the misuse of private data. For example, if an SME's customer database stored in a Cloud is

compromised, it can lead to the exposure of customer's personal information, and in the worst case can lead to full identity theft [27] [28]. Therefore, while Cloud storage makes it easy to save and share files, and minimize IT cost, it also leads to more IT security vulnerabilities.

Prevention: SMEs have to be careful with who can access the stored data, and they can use built in security solution like encrypting data before storing into cloud [55]. There are many scientific researches in development describing prevention methods. [46]

2.7 BYOD

The availability of 3/4G internet accessibility and smart devices like laptops, tablets, smart phones, etc. has introduced a sudden growth of device mobility trends. Part of the mobility trend is BYOD (Bring Your Own Device) that means the employees use their own devices during their working time. The more recent term "Bring Your Own Technology" (BYOT) is replacing the term "Bring Your Own Device" (BYOD), which generally includes both hardware and software.

BYOD (or BYOT) is common in many businesses. According to the Cisco survey performed in the US in 2012 among 600 U.S. IT and business experts, 95 percent of respondents said that their organizations allow employees to use their own devices in workplace [19]. That same survey led to the estimation that the average employee with technical background uses 2.8 connected devices at work, and the number of connected devices per employee is expected to rise in future. A survey stated that in Europe an increasing number of companies are allowing BYOD [18] However, there are still some hesitations about security problems occurring from employees connecting personal devices to company resources [18].

Advantages: These changing habits of BYOD bring opportunities for the enterprises. The opportunity is related to two main characteristics: increase of productivity of the employee and the cost reduction. For BYOD, during work employees can be comfortable with using their own devices. Also in a BYOD, the employees pay the full or partial cost of purchasing and maintaining the devices, which reduces organization's IT cost.

BYOD as a Threat: BYOD also brings some critical risks. The threat agent in BYOD is the employee or the insider. In literature, insider is an employee who is authorized to use a particular system or facility of a company [49]. Few studies [43], [34] have focused on the insider abuse threat in companies. Insider may pose a threat to an organization because of his/her unawareness, faults, and deliberate acts [50] [51]. According to a CSI/FBI survey [52] that was conducted among 616 computer security practitioners in the USA, 64 percent of the respondents reported that some of the losses related to information security have incurred due to the actions of insiders. For example, an insider may cause IT security threat by unknowingly retrieving spam, opening a virus infected e-mail attachments or dismissing information security threats as insignificant [53]. The 2013 Norton Report [3], which conducted a survey among random samples of 13,022 online adults across 24 countries, stated that:

- 49% use their personal devices (PCs, laptops, smart phones, and tablets) for work-related activities.
- Nearly half does not use basic precautions such as passwords and security software. Only 26% of Smartphone users have mobile security software with advanced protection, whether 57% are not aware that security solutions for mobile devices exist.
- 27% have lost their mobile device or had it stolen.

Portable devices (smartphone, laptop, and tablet) users are likely to use devices' features and apps [17]. For using the device's features an employee can connect personal devices to unknown or unsafe networks or machines (can be both wired or wireless); and can be infected with malware, virus or some malicious scripts. When the device again connects to the company network, this connection can open a path for malware, spyware, virus or script to migrate from the personal device into the company's machines and over the company's networks. This shows how only one personal device can affect the whole company IT infrastructure.

In the other direction, sensitive official data can be saved on the personal devices. This can be even in a form of an email attachment retrieved in the device. This data can include private customer information and proprietary company information. Even one random stolen device, which stored company information, can disclose sensitive information about that company [20].

Prevention: The best way to address BYOD threats is through explicit policies such as specifying permitted personal devices, specifying service like which application can be used in BYOD device, etc. The organization should decide to which extent it will allow its employees to use BYOD. The organization determines what devices employees are allowed on the network and generates policies stating appropriate devices and acceptable behaviors. Technical control like the use of MDM (Mobile Device Management) software can also help the organization to reduce BYOD threats [10].

Cloud Computing and BYOD threats are seemed to be severe; they can be tackled by enforcing a few policies on employee behaviors of using these technologies. For example, BYOD threats are solely based on the user's activity with his/her personal

devices. Therefore, enforcing policies on how to use personal devices with sensitive official information can solve the problem. Besides, all the Cloud Computing threats are there because of the sensitivity of data that can be leaked. If there are few common practices related to saving data in the Cloud in a secured manner, this threat can be mitigated. Table 5 describes the Cloud Computing and BYOD at a glimpse.

The top ten security threats, along with BYOD and Cloud Computing trends have made SMES vulnerable to high-impact security events of cybercrime. Businesses of all sizes must prepare for these threats. Moreover, there is no research on security measures existing in SMEs in Europe against BYOD and Cloud computing security threats. This leaves us predicting few expectations about the security scenarios of SMEs in Europe. In addition, there is no scientific research based on employee's behavior on using Cloud computing and BYOD. Therefore, the recent researches about the prevailing practices about BYOD and Cloud Computing in an SME, there is enough room for research on these topics.

Table 5 Cloud Computing and BYOD at a Glance

Category	Cloud Computing	BYOD
Definition	Cloud Computing stores data and software on remote servers and provides customer access to them via the Internet. The customers do not have to store data, software, or processing power on their own computer,	BYOD (Bring Your Own Device) that means the employees use their own devices during their working time.

Advantages	Offers all the functionality of current information technology services and reduces the costs of computing. It helps the SMEs to decrease their expense and time on IT field [54].	Increase of productivity of the employee and the cost reduction for the company
Disadvantages	• The outsourcing of data to Cloud introduces risks like poaching, the theft of intellectual property, proprietary software, and critical confidential data [55] [56] [57] [58]. • Cloud service providers can misuse of private data and uncover secret plans, designs or strategies of a customer of an SME stored on Cloud.	• Personal portable devices used for work can be stolen, thus exposing sensitive official data. • Personal devices can contain virus, malware that can affect the company's network. • Unknowingly retrieving spam, opening a virus infected e-mail attachments in devices.

Prevention	**SMEs Preventive Action** Implement a policy of securely using Cloud for work. For example, using Https for connection. **Individual Preventive Action** • Be careful with who can access the stored data. • Encryption of data before storing into cloud [55].	**SMEs Preventive Action** • Implement explicit policies. For example, specifying permitted personal devices, application can be used in BYOD devices • Generate polices stating appropriate devices and acceptable behaviors of BYOD. • Technical control like the use of MDM (Mobile Device Management) software can reduce BYOD threats [10].

2.8 STUDIES RELATED TO CYBERCRIME IN SMES

Cybercrime and IT security are widely researched topics by governmental authorities, scientific research organizations, company related to IT security products and other non-scientific organizations. Among these organizations, companies related to IT security products who conducts these kind of studies limit their research on the IT security threats their product prevents; and provide commercial solutions to these security threats only. Commercial studies have limited scientific usefulness due to the lack of control cases they use for the research. However, commercial studies can be a great source of

information for the huge number of respondent they have. In this study, both commercial and scientific sources have been covered.

2.8.1 CYBERCRIME STUDIES WITH RESPECT TO GREY PAPERS

Several commercial/grey surveys have brought on account of this inquiry. The good thing about grey studies is they talk about the monetary loss of cybercrime in the organizational environment. In Table 6, these commercial/grey studies are presented. These studies are chosen for this research because these surveys have taken samples related to:

1. A respondent who is working/owning Small Medium Enterprises.
2. A respondent who is an IT professional/expert.
3. A respondent who is a security expert.
4. Recent studies (only the surveys conducted in 2012 and 2013).
5. Monetary loss related to cybercrime.

As from Table 6, most of the surveys (like the Australian CERTs cybercrime survey [7]) have sample data from large well-known organizations. There are few recent surveys based on North American countries (USA and Canada) like [2], [8], [9] and Australia [7]. Surveys like [2] and [8] are deployed by governmental agencies. Those surveys tried to assess the current cybercrime situation, and victimization cost sampling both general adult and security expert. Moreover, studies like [7] and [9] are deployed by nonprofit organization trying to ascertain the strength of IT security policy and measures among SMEs.

As shown Table 6, there is one recent survey conducted in SMEs operating in Europe. This gives the scope of research as the current state of IT security on SMEs based in

Europe. Some of these studies [3], [6] are purely commercial and their research questions are based on the security solution they sell and the solution's effectiveness. The studies described in Table 6 have only focused on the current scenarios of the organization. However, these studies do not cover the reasons of low protection measure against cybercrime on SME environment.

Table 6 Examples of surveys conducted by different organizations (Grey review)

Reference	Conducting Organization	Year	Data Collection	No of Respondents	Types of Respondents	Country Approached	Important Key Facts
[3]	Norton/Symantec	2013	Online survey	13,022	Adult	24 countries all over the world	The consumer is using mobile devices and merging work and personal devices into one. Global direct cost of cybercrime is 113 Billion US dollars.
[2]	FBI and NW3C	2012	Cybercrime victims complaints	289,874	US citizens	USA	Adjusted dollar loss of total cybercrime victimization is $525,441,110
[6]	Kaspersky	2013	Online interviews	2,895	IT professionals	24 countries all over the world	IT security is the main concern of IT management of an organization; highlighted the use of a personal mobile device at work, and data leakage through insiders.
[8]	US Secret Service and CERT USA	2013	Online survey	500	Executives and security experts	USA	The results reflect the effect of insider attacks on organizations. Results conclude insider attack is worse than outside attack.
[7]	CERT Australia	2012	Online survey	255	Companies working in different sectors	Australia	Highlights the current cyber security measures, the recent cyber incidents victimization faced by organizations of Australia.
[9]	ICSPA	2012	Telephone interview	520	Small, medium and large Canadian businesses	Canada	Highlights the cybercrime situation in Canadian business operation. Finding includes different cybercrime threats victimization and their approaches to tackle them.

2.8.2 CYBERCRIME STUDIES WITH RESPECT TO PEER REVIEW

The scientific research/peer review done in this area has a varied purpose. For this research, the reviewed scientific papers have been limited to, different surveys carried by other peer researchers. Most of the surveys have addressed the facts about the reasons for the SMEs low cyber security practice. The researches that included the reasons for cybersecurity in SME and different survey conducted by peer researchers are listed in Table 7. Below the peer reviews are briefly discussed.

Some studies have reasoned that not having proper knowledge about the cybercrime can be a reason for low cyber security practices. SMEs in developed countries usually has a weak understanding of information security, security technologies and control methods. SME owners do not have sufficient awareness of information security [61] [62]. Firms often fail to understand why IT or cyber security is important [6, 41]. According to the 2013 US State of Cybercrime Survey [8] which was conducted on 500 executives and security experts stated that, many leaders/CEOs of SMEs underestimate their cyber-adversaries' capabilities and the strategic financial, reputational, and regulatory risks they pose. For SMEs, investing in security does not provide clear, measurable profits besides the perception of security.

While other studies have pointed out the high cybercrime prevention cost behind the lack of cybersecurity. Sometimes, SME owners do not pay attention to cyber security. For example, Johnson and Koch [50] stated that small SMEs would not pay for security. SMEs frequently use power surge protectors, but they are not likely to set up encryption and access control technologies [23].

The high cost of cybercrime prevention occurs, as the IT Security is not a one-time investment. According to the ENISA Threat Landscape Report Mid-year 2013 [22], the IT security threat range is very dynamic, so the adaptation and modification of IT security should be continuous. For example, offenders are now using cloud services to distribute their malicious payloads, which was not common few years ago. Another example can be the rise of denial-of-service attacks, which might be linked to hactivism [43]. Hactivism refers to a large group of motivated but unskilled individuals [46] executing a cyber-attack. Whereas, a few years ago few skilled individuals executed cyber-attacks, now executing cybercrime with the help of mass unskilled individuals is possible.

Lastly, few studies suggested that the reason behind poor attention to IT security could be SME's disregard to risk assessment and commercial guidelines. SMEs tend to neglect periodic or any sort of risk assessment to implement security policy [21] [40] [44] [46]. The reasons behind this behavior can be lack of funds, lack of time to protect against cyber security or inability to offer an appropriate level of information security awareness, training and education [23] [43] [51]. Although there are a number of policies and guidelines exist for organizations, to provide directions to information security. The commercial standard ISO-27000 [48] series helps to build structures of a firm's security policy. Especially ISO-270002 (security controls), ISO-270031 (business continuity) and ISO-270032 (cyber security) are relevant to SMEs. However, these guidelines are not practiced in SME for their high cost of implementation.

Few papers discussed about the low exposure of cybercrime. An information security breach is not often publicized in the SMEs industry environment. SMEs owners do not get many reports related to information security, because victimized organizations do not

disclose this information for reputational damage. This makes information security seem insignificant and draws less management consideration and support [23]. Finally, SMEs do not distinguish IT as connected to business strategy and may trust the security technologies, which are already being used in the business [24]. SMEs does not want to adopt to the new IT security technology. Sticking to the old security technologies does not help SMEs to protect against the latest IT security threats. This makes SMEs more vulnerable to cyber-attack.

As we can see table 7, there are as well not many researches done on cybercrime scenarios in SMEs based in Europe. In addition, none of these researches are focused on the latest IT security threats. An efficient environment for information security cannot rely solely on technical solutions [64]. Considering the high monetary cost of cybercrime prevention, it is time to focus on simple imposed rule and policy employee's behaviors and practice that can protect from cybercrime on SMEs. Moreover, the most suitable IT security culture can be insured by the cautious and good actions of employees [61]. As well, the low level of cybercrime exposure conceals the true alarming cyber-attack picture and leaves SMEs being unaware of the cybercrime threats they are facing every day.

Table 7 Summary of the studies (peer reviews) on surveys of SME's IT security trend

Reference	Year	Data Collection	No of Respondents	Types of Respondents	Type of Organization	Country	Survey Focus
[38]	2004	By hand and email	121	IT security personnel	SME and big organizations	USA and Europe (Mainly UK)	Specific security practices and risk assessments in organization.
[42]	2006	Online survey	232	Business owner.	Home-based small business	USA	Attitudes toward specific computer security risks and the self-reported defenses taken by small business owners.
[39]	2005	Via email	138	Business owner	Small business	USA	IT related security issues in small firms and provide direction in planning, training, and exploitation of IT.
[34]	2004	Online survey	50	IT professionals	Different industry sectors	Europe (70% from UK)	Insider misuse of IT and its consequent impacts upon the organizations.
[61]	2007	Case study	3	All the employees of the three organizations	Small business	Australia	Information security culture, employee behavior and SME owner's awareness of information security and risk.
[65]	2012	Hands on interview	157	Employees	Different industry sectors	Slovenia	The impact of security culture characteristics, on the behavior of employee regarding security.
[69]	2013	Interview	110	Employees	Small Medium Enterprise	Malaysia	Information security awareness among employees without technical background.

2.9 DISCUSSION

In the literature, the study discussed the most significant IT security threats and its related impact on SMEs. This research will primarily target SMEs based in Europe. The questions of the research focus on the security of IT assets and information sharing in the Cloud.

The asset of an SME varies depending on its business activity. The threat varies as well, depending on the relevant assets. Therefore, these assets are crucial to define the potential security risks related to it [48]. For this research, the assets of an SME are limited to servers, desktops, laptops, mobile devices, information shared in the cloud and email system, because those are the common assets for most SMEs conducting business operation online. The research questions will be also cover different policies of using these assets.

More specifically, this research will focus on the following issues:

1. Potential security risks related to Cloud Computing and BYOD in SMEs.
2. Cybercrime prevention measures related to BYOD, Cloud Computing and general IT security threats.
3. The awareness of cybercrime and IT security measures of SMEs.

The expectations of the results of the survey are based on security threats, prevention measures, IT knowledge of the employees, BYOD and Cloud Computing. Expectations of the results of the survey for this research are:

Expectation 1: An SME with fewer employees is less likely to have IT security measures and policies.

Expectation 2: Most SMEs do not have policies for BYOD and Cloud Computing.

Expectation 3: SMEs selling non-technical products with the non-technical employee background are supposed to be the most vulnerable to cybercrime.

Expectation 4: SMEs selling technical products with the technical employee background are supposed to be the least vulnerable to cybercrime.

Expectation 1 is based on Johnson and Koch [50] statement about small SMEs (which indicates smaller number of employees) would not pay for IT security mentioned in 1. Also mentioned in the 1.1 SME owners do not have sufficient awareness of IT security [61] [62]. This gives the basis of Expectation 2, 3 and 4. An employee's sufficient awareness/knowledge of IT security must be linked to his/her background in IT. So Expectation 3 and 4 are based on the IT background of employees and their knowledge to cybercrime prevention measures. The idea of "least" or "most" vulnerable to cybercrime based on the frequency of victimization suffered by SMEs.

3. METHOD

The study is conducted in five phases with particular focus on small businesses - that is, firms with maximum 250 employees [29]. In phase one, by reviewing and synthesizing relevant literatures, a preliminary conceptual idea about the most important aspects of SME's IT operation was developed. In phase two, a questionnaire is built to ask questions related to the Expectations based on the CERT Australia 2012 [7] and Dirk Sikkel's report for SIXTAT [60]. In phase three, pilot interviews were conducted to test the questionnaire. Two SMEs were interviewed face to face, and one SME was interviewed over the telephone. The questionnaire was modified after the pilot interview phase to

make it simpler by describing all the technical terms. Therefore, any employee in SMEs, irrespective of his/her technical background can answer the questionnaire about IT security measures of SMEs. In phase four, more European SMEs were interviewed. In phase five, the survey was conducted online, to reach more SMEs all over the Europe to have a vivid and comparable data based on geographic locations.

3.1 RESEARCH SAMPLE

SMEs are divided in categories based on the products they sell and the background of technical studies their employees have.

SME selling non-technical product with the majority of **non-technical employee** can be a home based jewellery shop described in 2.3 SME scenario 1. **SME selling non-technical product** with the technical employee is expected for a company, whose employees have a technical degree or training. An example can be a car repairing garage described in 2.3 SME scenario 2. For **SME selling non-technical product**, IT security is expected to be outsourced, also the number of employees working in IT in this organization is expected to be low.

An SME selling technical product with technical employee can be any software solution provider described in 2.3 SME scenario 3. Here most of the employees have a technical background, all security activities are expected to be carried out in the company. **SME selling technical products with non-technical employee** can be a consultancy firm providing online accounting tools for the clients. For this type of SME, employees are expected to have non-technical background.

For this research, 10 SMEs from each category will be interviewed from each category unbiased data. The survey population is SMEs and it is difficult to find a large number of respondents in a short period of research. Therefore, even the research does not find enough number of samples to provide a meaningful data; it is enough to test the questionnaire to take the study further for the future researchers. Table 8 describes the category of survey respondents.

Table 8: Categories of Survey Respondents

	SME with non-technical employee	SME with technical employee
SME selling non-technical product	10	10
SME selling technical product	10	10

3.2 SURVEY DESCRIPTION

The questionnaire has been designed in English. According to the Special Eurobarometer of the European Commission [30], English is the most widely spoken languages in addition to the mother tongue. Most of the questions are multiple-choice with carefully chosen options. However, open fields are included in the questionnaire, so the respondent can provide more information. The questionnaire is expected to be filled in by a designated person within the SMEs who deals with the IT and other main operations of the SMEs (most preferably the CEO/CTO/COO or CFO of the SME).

It can be uncomfortable for the firms to disclose if they were ever victim of cybercrime. For that purpose, anonymity has been guaranteed to the respondents to get honest and hesitant free responses. For the purpose of the research, a non-disclosure agreement/ consent form was provided to the respondents signed by the researcher stating that, no name (both firm and the respondent's) would ever be mentioned anywhere in the study. This guarantees full anonymity of the respondents. In the online survey, reading and signing the consent form is the first step to start the survey. The questionnaire/survey contains no mandatory question. This provides flexibility to the respondent to answer to all the questions being in his/her comfort zone. Any respondent can forward the online survey to other interested parties.

The survey consisted of several questions, both closed and open ended, to ascertain:

- Business description
- Types of IT security used
- Detailed description of BYOD (Bring Your Own Device) and Cloud Computing
- Types of cyber security incidents experienced
- Personal view about current IT security measures.

3.2.1 DATA COLLECTION PROCEDURE

The best way to collect information from SMEs for the survey is by face-to-face interview. Based on the literature review, a questionnaire is designed to prompt questions about IT infrastructure, the technological trend and security policies in SMEs. The problem with researching on SMEs IT security detail is that they are not open to disclose their business operations and security measures [59]. In addition, the response of SMEs

to any survey is usually very low [59]. Considering all the limitations, conducting survey in interview manner is the best way to collect quality data from SMEs.

The survey was conducted in both interview and online survey manner. At the beginning of the data collection phase, ten interviews were conducted over the period of March 2014 until April 2014. The respondent SMEs were chosen randomly, and they are based in Netherlands, Austria and UK. Eight Interviews were conducted over the telephone, which lasted approximately twenty minutes. Rest two interviews were conducted face to face, which took almost thirty-five minute. The respondents were given the opportunity to terminate the interview anytime, or skip answering questions they were not comfortable with. Although face-to-face interviews are very good for collecting high quality responses, this interview process took up a lot of time for both the researcher and the SME to plan and set up a meeting and were therefore discarded as an option for this study.

The ideal choice for surveying SMEs in terms of time consumption is an online questionnaire. The SME respondents can fill it in at any time that suit them the best and it takes up significantly less time than a spoken interview. A difficulty with this type of interview lies with the questions of the questionnaire, they need to be more accurate than a face-to-face interview, as the interviewer cannot add information to put the question into context or ask follow-up questions.

In the second phase of the data collection phase, an online questionnaire was chosen to gather the needed information from as many SMEs as possible. In the beginning of the online data collection phase, another student working on the similar topic of cybercrime in SMEs collaborated with this project to gather more respondents for the study. For this

collaboration, both Dutch and English version of this questionnaire was made and distributed. Six respondents participated in the Dutch online questionnaire. In addition, during the second phase of data collection, the survey was put in Google as an advertisement of cybersecurity survey to increase the number of responses. The advertisement was live in Google for seven days. Unfortunately, this attempt did not get any valid full response from SMEs during the seven-day period.

3.2.2 MEASURES

The study wants to compare the IT security measures taken by an SME and the cybercrime victimization incidents. The procedure of measuring an SME's vulnerability depends on the security measures it has with regard to the current security threats, also associated policies implemented in the SME as prevention. Incidents and security measures can be placed in multiple categories. Categories that have discussed in this paper are described below.

SME: The business organization that has been focused in this study are Small Medium Enterprise and its annual turnover and employee have to follow a certain limit.
Facts that help to determine an SME are the number of employees and the annual turnover. In addition, the age of the business and the employee's educational background were considered in the study.

Categorizing SMEs: Respondent SMEs are asked to categorize themselves based on the business operation they are in or the type of product they sell. The SMEs are categorized in technical SME or IT SME and non-technical SME or non IT SME. As well the

respondent SMEs were asked to see what portion of their employees receive any form of technical educational background.

IT Security Technology: To assess the protection against cybercrime victimization, SMEs are asked to determine the security measures they have employed in their office. The security measures have been categorized according to the type of protection they offer or the threats they tackle. Incidents and security measures are categorized in the following topics:

Virus/Malware/Spam/Phishing: These types of security technology prevent exploitation of the IT-infrastructure caused my malicious script, illegally downloaded software or even deliberate email by third parties. The best known example in this category is the anti-virus/spam/phishing software that scans the system(s) for viruses, spam and prevents phishing email.

Hacking: These types of security technology prevent attacks from the intrusion of outsiders from unauthorized access to the company's IT infrastructure. A firewall is a technology that is commonly applied to prevent hacking. Types of hacking can be defacement of the company's website by attackers.

Compromised data: These types of security technologies prevent data breaches to parties outside of the company. An example of this kind of security measures is encryption of data, using a secure connection of browser, encrypting USB media content, etc. In case of encryption, encrypted data transfers in the Internet so nobody cannot monitor the transmitted data. As well, stolen media content (i.e. USB flash drive) would not be usable to anyone other than the authorized person for encryption.

IT Security Policies: The absence of IT security policies is one of the ways in which lack of cyber security can be manifested. IT security policies are formally

written/documented security policies. IT security policies define issues such as the IT security goals of the organization, what specifications and guidelines need to be followed, and therefore what is acceptable and what is not acceptable in the organization [35].
IT security policies that have been addressed in this study mostly focus on BYOD and Cloud computing threat prevention policies. Other policies that have been addressed are control against the pirated software and involvement of the third party organization in ensuring IT security. In addition, this study wanted to find out if formally documented security policies are common in SME with respect to its employee number.

BYOD Scenarios: The adaptation of BYOD trend by SMEs based in Europe have investigated this the study. BYOD policy specifies a number of information security controls applicable to the use of mobile and portable devices. Employees who prefer to use their personally-owned IT equipment for work purposes must be explicitly advised by the BYOD policy to follow certain rules. These BYOD rules must secure official data to the same extent as an official IT equipment, and must not introduce unacceptable risks (such as malware, stolen devices, data leak etc.) onto the networks by failing to secure their own equipment.
For assessing the BYOD security the following topics are put into consideration: if the company allows BYOD, if the company has some BYOD policy and what does this policy cover and finally how the company tackles the security threat of lost or stolen BYOD. Best practices for an SME having a well-defined policy for BYOD and taking measures for lost BYOD.

Cloud Computing Security: This study wants to investigate the role of cloud computing among SMEs in Europe. Cloud Computing topics that have been addressed in this study are: based on SME's need, what kind of cloud computing service it uses, if the SME ever

suffered from any cybercrime victimization due to Cloud Computing, and how the SME is trying to protect itself from Cloud Computing related threats. SME is considered to have better protection against Cloud Computing threats if it is using encrypted session (Https) to the Internet, if the Cloud is a matter of audit and monitoring how often this audit and monitoring works etc.

Cybercrime: SME's vulnerability to cybercrime can be determined by the number of cybercrime victimization incidents the SME encountered. The cybercrime incidents that have been covered in this study are related to Virus/malware attack, hacking, compromised data, BYOD and Cloud computing incidents. In addition, if an SME is a victim of a cybercrime, it asks questions about the estimated number of experienced IT security related incidents, and which organization (i.e. Police or government agency) it contacted for this matter.

3.2.3 CONCEPTS

To answer the research questions proposed in the study, few questions were included in the questionnaire to assess the IT security measures taken by SMEs, the cybercrime victimization and the opinion of the respondents about cybercrime. Along with the question sections dedicated to BYOD and Cloud Computing, the following questions served the purpose:

Q16: Which cybersecurity policies in your company are in place at the moment?
Is it yet common among the SMEs with less number of employees, to have security policies. Likewise, if there is a written policy for the purpose of the employee's assets (portable device of the employee), what does this policy actually cover. This question

was included to assess the policy side of IT security measures within the SMEs. The answers include policy related to BYOD, Cloud Computing, control against the pirated software, having formal/documented computer security policies etc.

Q18: Over the last 12-month period (2013-2014), which of the following technologies are being used in your company for IT security purposes?

This question was included to assess the usage of IT security technologies in the SME. The answers include security technology like antivirus/-malware protection, encrypted login/sessions (SSL/HTTPS), encrypted files etc.

Q28. Over the last 12 month-period (2013-2014), has using a BYOD for official purposes caused any of the following problems.

This question was included to assess the victimization related to BYOD in particular. BYOD threats can be occurred from different types of incidents, and the question tries to figure out which incident cause the BYOD threats. The incidents are consisted of stolen device, retrieved message in a device and the presence of virus, malware etc. in a personal device.

Q38: Over the last 12 month-period (2013-2014), which of these IT security related incidents has your company faced so far?

To assess the cybercrime victimization for the SME, this question was included to identify the types of incidents made SME suffer. The answer choices provided for this question covers security incidents related to virus/malware, hacking and compromised data as explained in "IT security Technology" in section 3.3.2. These particular security incidents are covered so if any SME is victimized of these incidents, there can be a

relation between the security technology SME use and the corresponding cybercrime victimization.

Q68. Do you think that the cyber security risks in the SME business environment are increasing?

This question was posed to find out SME respondent's view about cybercrime. An open box is included in the answer field to put a comment about the respondent's view to cybercrime. This question will reflect what SME believes about cybercrime and how correct the SME is about the current cybercrime situation.

4. RESULT

4.1 SAMPLE DESCRIPTION

After a period (March 2014 till May 2014) of gathering respondents, a total of 17 SMEs filled in the questionnaire. One of the respondents was omitted from the results on account of its number of employees being too high to be considered as an SME [33]. Out of the 16 valid respondents, ten respondents were interviewed and six filled out the Dutch online questionnaire. The sample within the defined population consists of application developers, security solution provider, accounting firm, IT consulting firm, garage owner, hospitality and medical service provider. Age of the SMEs ranges from 3 years to 20 years.

Although the study initially wanted to categorize SME based on both business performance and IT background of the employees (see Table 8), due to lower number of samples, the SMEs were divided only based on their business operation (IT and non IT). IT SMEs are the one selling technical product, and non-IT SME are the one selling non-

technical product. As shown in Table 9, a small majority of the SMEs identified themselves as an IT company (56%). This is derived from question 4 in the questionnaire. The sizes of the SMEs varied a lot, but the majority of SMEs has a number of employees ranging from 5 to 49 as can be said from Table 10

Table 9 Types of SME Respondents

SME Types	Respondent Percentage
IT SME	56%
Non-IT SME	38%
Other	6%

Table 10 Number of employees of the respondents

Number of Employees	Number of Respondents	Cumulative Sample
2 to 4	3	3
5 to 9	5	8
10 to 19	2	10
20 to 49	5	15
50 to 249	1	**N**= 16

4.2 SURVEY RESULTS

This study gathered data from 16 respondents. Among the 16 respondents, 10 of them were interviewed by the resercher. While interviewing, the study got a chance to gather some of the respondent's personal views and opinions about the answers they provided. In this section, the study frame the emerged categories as narratives using

interview extracts that include views related to cybercrime, IT security protection, etc. This study also includes a respective quantitative measure of each concept along with the narratives. Some of these narratives has been rephrased for the sake of better understanding.

IT Security Technology: SMEs were asked what type of computer security technology they used in the period of 2013-2014. 13 out of 16 respondents (over 80% of the respondents) reported using antivirus/-malware, Firewalls, Anti-spam/phishing, Virtual Private Networks (VPN). 10 out of 16 respondents (over 60% of the respondents) also reported using Encrypted login/sessions (SSL/HTTPS) for browsers. Firewalls and spam filters are not always effective in preventing or detecting sophisticated attacks, so the use of intrusion detection systems (IDS) is quite noticeable. 7 out of 16 respondents (almost 43% of the total respondents) reported using a type of IDS. 8 out of 16 respondents (50% of the total respondents) reported their use of legal software. 5 out of 16 respondents (over 30% of the total respondents) reported using access control using biometrics, smartcards and tokens and keeping off-site backups. For example, one of the respondents stated about the usage of IT security technology:
"We use open source software and our own private cloud. We do not like to outsource anything. And open source operating system and software, are way better than using proprietary software."

The preference of using the open source software over the proprietary software has few reasons. Open source software is free and it does not have a problem like being illegal copies of the software. In that context, using the open source operating system and software can provide better and cheaper security for SMEs. Using open source software and operating system can save SMEs from the problem of controlling employees for

using illegal software. As one of the respondents admitted that, they have no way to control employees from using pirated software in the workplace.

"Unfortunately, we don't have anyone who will take care of employee's laptop checking if they have pirated software installed. We still encourage them not to use illegal software."

Figure 1 provides a breakdown of the security technology being used by the respondents. Figure 1 also includes and compares this study's result with the result of Cert Australia's [7] result, which surveyed 255 organizations (large enterprises) of various sectors in Australia. For the purpose of this study, there are different types of security technologies included in this chart other than the CERT Australia report. In Figure 1, those security technology options that contain null or no value for the CERT Australia result were not discussed in the report CERT Australia report [7].

Figure 1 shows that despite geographic variation, respondents in both continents have a similar attitude towards IT security technology. One fact that can be concluded from Figure 1, for every category of IT security technology, more respondents of Australian organizations use security technology than that of European SMEs. In using specific security technology, Australian organizations scored 10% to up to 30% more than that of European SMEs. This graph shows that more organizations in Australia use security technology than European SMEs. From Figure 1, it can be concluded that a greater number of large enterprises (sampled in the CERT Australia report [7]) use specific security technologies than SMEs (sampled in this study).

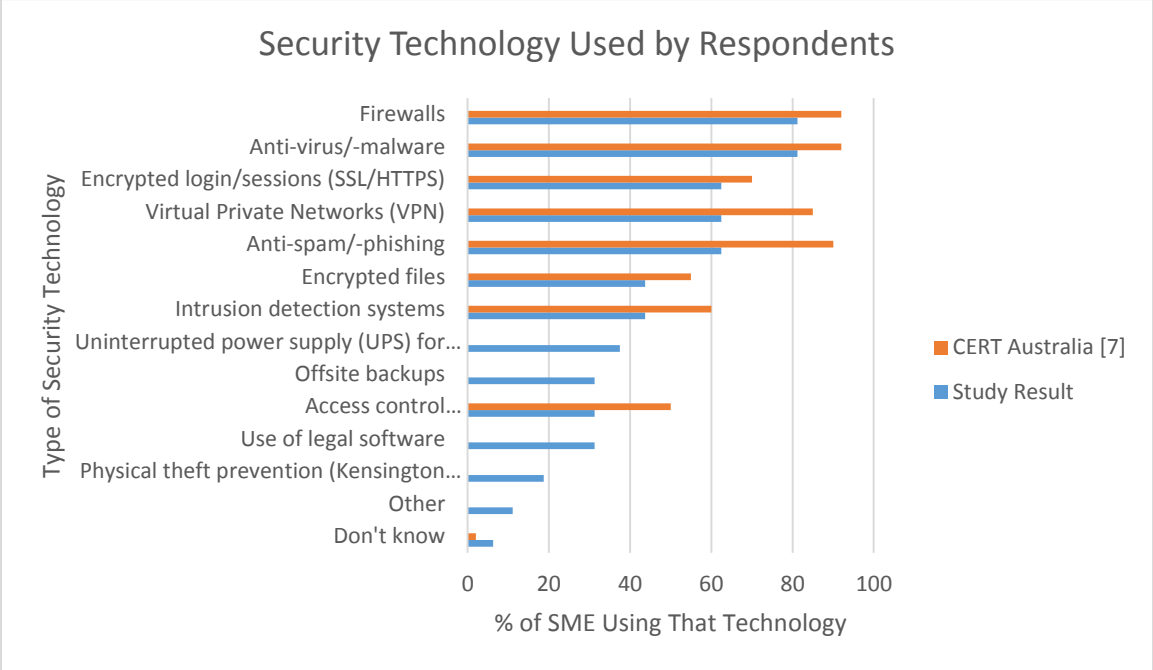

Figure 1 Security technology being used by respondents

IT Security Policy: Basic security policies are used among the majority of surveyed SMEs. For example, 11 out of 16 respondents (68.75% of the total respondents) perform media backup, 7 out of 16 respondents (44% of the total respondent) have formal/documented computer security standards and perform training of personnel in security procedures. The respondents claimed that even if they do not have a documented policy, there are always some unwritten guidelines about how to use different devices. For example, one respondent stated:

"Even if we don't have a written policy, we follow some unwritten rules."

Also, 90% of the respondents that provides security solutions and are application developer have formal/documented security policy. As well, the respondents who do not have a formal security policy have less than five employees. The reason behind this practice can be the intimate workplace environment for less number of employees. It is

expected to have better employee communication inside an SME with less number of employees. One of the respondents stated:
"We are a very small company, there is no need to have a written policy. You can always tell your colleagues in person what to do."

5 out of 16 respondents (31% of the total respondents) have plans in place for the management of removable computer media, such as USB memory drives. Although a good number of 8 out of 16 respondents (50% of the total respondents) has policies related to Cloud Computing security, and 7 out of 16 respondents (almost 43% of the total respondents) has policies relating safety of using a personal device for work. Figure 2 provides a detailed breakdown of the security policies used by respondents.

Like Figure 1, Figure 2 also includes and compares this study's result with the result of Cert Australia's [7] result. There are different types of security policies included in Figure 2 other than to the CERT Australia report. The security policy options, which contains null or no value for the CERT Australia result in Figure 2, were not discussed in the CERT Australia report [7].

Figure 2 shows that respondents in both continents have a similar response towards IT security policies. Also in Figure 2, every category of IT security policy, more respondents of Australian organizations uses a particular security policy than that of European SMEs. In using specific security policy, Australian organizations scored 10% to up to 40% (policies related to having formal documented policies, business continuity plan and computer monitoring center) to a greater extent than that of European SMEs. This graph shows that more organizations in Australia paid attention to formulate a security policy than European SMEs. From Figure 2, it can be concluded that greater number of large

enterprises (sampled in CERT Australia report [7]) use and formulate specific security policies than SMEs (sampled in this study).

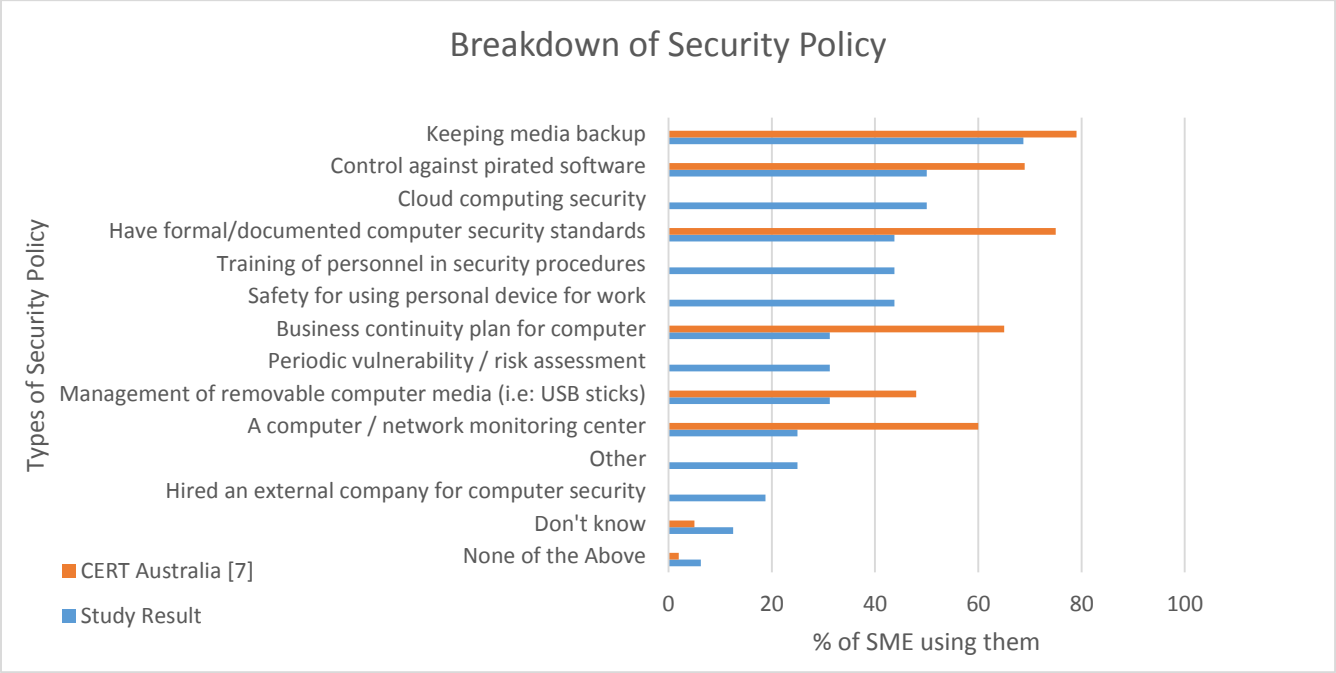

Figure 2 Breakdown of Security Policy adopted in SMEs

BYOD Scenario: To investigate the BYOD trend in SME, the questionnaire asked questions about the adaptation of BYOD and security threats related to it. 10 out of 16 respondents (almost 62% of the total respondents) said BYOD is allowed in the company. One of the respondents stated:

"BYOD threats will not be severe in our case as most of their employees have an IT background, and they know all IT security procedures".

This might indicate that the management/employer trusts the employees with IT background to use devices more cautiously, expect the employees will know the IT security threats related to BYOD, and act carefully. One of the respondents, who falls in

the category of IT SME, stated all of their employees use BYOD, and they are very confident that their employees are aware of the BYOD security threats as they all have some IT background.

"BYOD is not increasing in our company, BYOD reached its maximum in our company; and everyone works with their own laptop in office."

The rest 6 out of 10 respondents (rest 38% of the total respondents) who did not allow BYOD stated they provide laptops for their employees as BYOD might reduce their organization's IT security. BYOD related problems could occur through a stolen device. None of the respondents faced any BYOD related security problem so far. However, 6 out of 16 respondents (irrespective to allowing BYOD or not) have hands on security protection in case any device is stolen. That security measure enables SME to remotely wipe out the information of the stolen device.

Cloud Computing Security: The study also wanted to investigate how cloud computing technology being used in SME. The survey stated 10 out of 16 respondents (62% of the respondents) use commercial Cloud and 3 out of 10 Cloud Computing users stated they use private Cloud for the confidentiality of their data. One of the private Cloud user respondents stated that the agreement of commercial Cloud lets the Cloud service provider save the customer data in the databases located outside of Europe, where might have different legislation for the Cloud service provider than Europe.

"As a company providing security solution to another company, confidentiality is our main business aspect. We do not even use the commercial Cloud service. Because the commercial Cloud service provider can access our saved data then."

Among the 62% of respondents who use commercial Cloud, 30% of them store the data in Cloud in an encrypted form. 90% of the respondents who use any sort of Cloud claim

to use secure connection (HTTPs) for connecting to the Cloud, which is a good security practice, as the login information to the cloud will be encrypted while transmitting. In addition, none of the respondents reported any security incident related to Cloud Computing.

Cybercrime: The questionnaire asked respondents about if they have experienced a cyber-security incident in the 2013-2014 period. 12 out 16 respondents (75% of the total respondent) said they did not experience any IT security related incident.
Among the 25% (4 respondents) who experienced security incidents, one of them stated: *"We faced Botnet attack before. There was no damage and the attack was prevented."* Two of the four victim respondents have reported they experienced Virus/malware attack and Spam/phishing mail, and one of them was hacked and the other's website was distorted (website defacement attack). These three respondents reported the number of incidents they experienced in 2013-2014 are in a range of 3 to 10.

Both of the SMEs who faced the website defacement and hacking incident contacted Police. However, the police could not help them out to catch the culprit who caused these incidents. This also indicates that it can be hard to find the attacker even by the police. This frustrating evidence shows that cybercrime attackers can be coveted and hard to bring under justice. The cybercrime attacker represents a considerable challenge to the law enforcement authorities. One of the respondents shared his frustration stating: *"The police could not help us to find the attacker. We filed a formal complaint for regulation, and provided the ip address of the attacker. But the police could not provide any more information about attacker."*

Additional Comments: The study asked few questions about the IT security management of the SME. These questions cover aspects like the budget of IT security of an SME and other monetary information about IT budget. The aim of these questions is figuring out how much SME tend to spend on IT and how much importance is given to the IT security. The responses incurred mixed results. As for most respondents, they could not provide an exact figurative answer for IT security budget, but could provide some insightful qualitative answers.

The study also asked if the SMEs are increasing the IT security expenditure in 2013-2014. 5 out of 16 respondents (32% of the total respondents) said they are increasing their IT expenditure. IT SMEs stated the obvious answer, that they spend their most of the budget on IT.

"Most of our budget is considered as IT budget"

In addition, this lead to the question, do the SMEs reserve percentage of IT budget for the IT security? As SMEs are small businesses and do not distinguish IT security cost different from regular IT cost. One of the respondents stated:

"We do not have any budget focusing solely on IT security budget. The normal cost of IT infrastructure can be our IT budget".

SMEs who are not increasing IT security, are mostly non-IT SMEs, these SMEs have outsourced their IT security to different third party companies. In addition, non-IT SME has dependency on IT service providers about IT related decisions for their companies.

"I don't think we need to spend more money on IT, we have everything we need. Although I don't know much about IT security. Whatever my IT service provider suggests, I approve that."

The SMEs were asked questions about their views about cybercrime in general. Most of the SMEs thinks cybercrime is increasing. One SME stated that the reason behind the increasing number of cybercrime could be SME's dependency on the Internet for business operation. In addition, SMEs are reluctant to believe that they can be the victim of cybercrime. One of the respondents stated:

"We are not the one who should worry about cybercrime. The Bank and other well-known organization should be worried."

This comment indicates SMEs consider themselves as insignificant targets for cybercrime. They believe cybercrime attacker can only be motivated for attacking bigger organization. This kind of belief is risky, because as mentioned before, four of the respondent SMEs experienced some sort of cybercrime victimization. One of the victim SMEs complaint to police about cybercrime, and the police could not help them find the attacker. This indicates that, contrary to what SMEs believe about they will not be targeted by cyber criminals, SMEs are in a position to be attacked as much as a normal big organization. The cybercrime victimization seems not common for SMEs compared to the big organization; the reason behind this is SME cybercrime victimization are never publicized as the big organizations. This decision of publicizing the cybercrime victimization can be abolished by the respective victim SME, as this can be a reputation damage to the business. One of the respondents stated:

"I think the cybercrime is increasing, but SMEs will not disclose if they have an attack. It will be such a bad image for their business. Their customer might not trust them anymore."

This indicates that, there is a chance that SMEs are being victimized by cybercrime, but they never disclose any information related to the victimization. This kind of behavior limits the proper attention cybercrime should get, also it does not let other SMEs to be careful of cybercrime threats.

4.3 EXPECTATIONS

Expectation 1: ***"An SME with fewer employees is less likely to have IT security measures and policies."***

To reach a conclusion for this expectation, the study need to find how many security technology being used in the SMEs and if there is any relation between the usage of security technology and SME's employee number. A problem rises up around how to aggregate the usage of security engineering. The comparison of the use of security technology based on the number of SME employees can be done in a few different ways. One way would be providing different weighted value to each of the security technologies, and then determine the weighted score of each respondent on its IT security measures. This way has the limitation that the IT security technologies are independent of each other. The different IT security technologies cannot be compared and weighted according to the service they provide. Another way of weighting IT security measures can be comparing the price of each measure. However, weighting security technology based on its commercial price is not a good option, because a few respondents use open source operating system and software, which is free. In addition, the price of the specific security technology does not guarantee better security than free IT security software. In the simplest way, this study decided to count the number of security technologies being used by the respondents which can be compared based on the number of employees SME have.

Table 11 shows the relation between the number of employees and average security technology being used in a company. From the Table 11, it can be concluded that the average number of security technologies increases with the number of employees. Although the employee group 20 to 49 has a sharp fall (5.5 in security technology) in the average number of security technology, the reason behind this sharp fall is the group 20 to 49 has only one sample/respondent. In addition, Table 11 shows the SMEs with the

least number of employees use the least security technologies (5 technology in average). This above discussion is **more likely to be aligned** with the **Expectation 1** "An SME with fewer employee is less likely to have IT security measures".

Table 11 Relation between the employee number and security technology

Number of Employees	Number of Samples	Cumulative Sample	Average Number of Security Technology Used by SME
2 to 4	3	3	5
5 to 9	5	8	7
10 to 19	2	10	8
20 to 49	5	15	5.5
50 to 249	1	**N**=16	6

If we focus on the formally documented policy (44% of the total respondents), all the respondents (7 of them have formal policy document) who falls in this category has more than five employees. In addition, Table 12 shows most of respondents having over 20 employees have the formal documented policy.

Table 12 Relation of Number of employees to formal document of SMEs

No of Employees	Documented Security Policy	No of Respondents Having Documented Policy
2 to 4	No	0
5 to 9	Yes	2
10 to 19	Yes	1
20 to 49	Yes	4

Table 12 gives the idea that the more the number of employees, it is more likely to have a formal documented security policy. This above discussion is **more likely to be aligned** with the **Expectation 1** "An SME with fewer employee is less likely to have IT security policies".

Expectation 2: ***"Most SMEs do not have policies for BYOD and cloud computing."***
As stated in the "**IT Security Policy**" section, 7 out of 16 respondents (almost 43% of the respondents) have policies related to personal device using for work. This policy mostly covers backup data on the personal device, use of HTTPs and not allowing employees to download risky applications in the personal devices that used for work. Only one respondent stated they use Mobile Device Management software. As most of the SMEs does not have a policy for BYOD (57% of the total respondents), this is **more likely to be aligned** with the part of **Expectation 2** "Most SMEs do not have policies for BYOD"**.**

In addition, in the "**IT Security Policy**" section, 50% of the SMEs have policies related to Cloud Computing. Therefore, the result of study related to Cloud Computing policy cannot provide a conclusion for the part of **Expectation 2** "Most SMEs do not have policies for Cloud Computing"**.** A good practice among most of the SMEs who use commercial Cloud is having policies for Cloud Computing.

Expectation 3 and 4:
Expectation 3: ***SMEs selling non-technical products with the non-technical employee background are supposed to be the most vulnerable to cybercrime.***
Expectation 4: ***SMEs selling technical products with the technical employee background are supposed to be the least vulnerable to cybercrime.***

Expectation 3 and 4 are based on deciding which type of SME (IT or non-IT) are more vulnerable to cybercrime. As it has been mentioned before, the measure of vulnerability can be decided by which type of SME was more victimized in cybercrime. As mentioned in 4.2 cybercrime section, the survey did not gather enough evidence of cybercrime victimization. Only four respondents confirmed cybercrime victimization. Two of them reported the incident is a normal Virus attack. Due to low evidence of cybercrime, it is not possible to draw any conclusion about vulnerability depending on the type of SME's business operation.

5. LIMITATION AND FUTURE WORK

This study lacked the resources and time to perform a more thorough research. It was really hard to find survey respondents. As the respondents were mostly the CEO or top level management employee, it was hard to schedule an interview time with them. The length of the questionnaire could have been a reason that SMEs approached for the online questionnaire in Google advertisement but did not complete it. Although covering all topics related to IT security technology, policy BYOD, Cloud Computing and incident related to them are four inter linked vast topics. A dedicated, smaller, questionnaire designed specifically for any two of the topics mentioned may have resulted in higher quality data. This questionnaire can be used by other project for studies related to cybercrime and IT security. For further research, a good way to ensure gathering a good quality data could be taking a longer survey period which is more than three months. This way, gathering information about security incident related to BYOD and Cloud Computing would be possible.

6. CONCLUSION

The goal of the research was to find a relation between the level of IT security and the business operation for SMEs. Although the study has a limited number of respondents, it proved a few facts. The findings can be summarized as follows:

IT security technology: Antivirus/Malware/Spam/Phishing are the most commonly used security technologies in SMEs. The Anti-virus/malware/spam are the most widely known type of IT security technologies, hence the result was obvious. The use of encrypted login sessions and keeping media backups are also indications of good IT practices. Nevertheless, the use of legal software was low. One of the good practices of IT security technology is using open source operating systems and software. However, open source software is not common among non-IT related businesses, as the user without technical background might find it hard to use. Compared to Australian SMEs, European SMEs fall behind in adopting IT security technologies. The number of large enterprises is higher than SMEs, in case of using specific security technology.

IT Security Policy: IT security policies are still not a common practice among SMEs. Less than half of the questioned SMEs have policies in place in the form of internal documents. SMEs that do not have documented policies claim to have verbal and undocumented rules for IT security measures and policies. SMEs reasoned the smaller number of employees for not having any formal documented security policy. IT SMEs paid more attention to formulate and document security policies. For those SMEs, the most common security policies are related to keeping media backups, Cloud Computing and personal device practices. In case of IT security policy, more Australian organization adopts IT security policy than the European SMEs. In case of using specific security technology, the number of large enterprises is higher than SMEs.

BYOD and Cloud Computing: BYOD is an accepted practice in SMEs. The management does not restrict employees to use any of their electronic devices in the workplace. At the same time, most of the SMEs have no strong policy for using personal devices at work (both written and verbal). **SMEs do not anticipate the threats in an uncontrolled use of BYOD.** Most of the SMEs did not take precaution measures like remotely wiping the stolen devices or use of Mobile Device Management software for BYOD threats. In their defense, the respondents stated the management trust their employees with their relevant IT background, to perceive the threats of BYOD and act cautiously. This attitude puts all the blames on the employees for BYOD threats victimization. Among the limited number of samples of this study, no SME faced BYOD security threats (i.e. stolen devices). Still the SMEs could be a little cautious and help the employees to set some rules for BYOD, therefore problem like a leakage of official sensitive information does not happen.

Cloud Computing is also a common practice in SMEs. **Most of the SMEs uses commercial Cloud**. A private Cloud is common among the IT SMEs that provide security solution as their business operation. Private Cloud has to be managed by the company who uses it. Therefore, using commercial Cloud is very practical for non-IT or small SMEs. None of the respondents faced any Cloud Computing related security threats. Regarding Cloud Computing security practices, commercial Cloud users save their data in Cloud in plain text. Simply encrypting the information while storing in the Cloud can mitigate the problem of disclosing official sensitive data to the Cloud service provider. The good news is, most of the respondents who use any types of Cloud (both commercial and private) use a Secure Connection (HTTPs) to the connecting to the Cloud via Internet.

Cybercrime: The study could not collect much data about the cybercrime incidents due to the lower number of respondents and lower cybercrime victimization incident among the limited samples. A very small amount of incidents was reported by the polled SMEs, which can be a good sign. At the same time, the absence of reported incidents doesn't mean there were no incidents. SMEs that reported cybercrime victimization, identified virus attack as the most usual problem. In addition, one of the respondents reported that their website was distorted. Website is important for SMEs as they connect with their customers via the website. The role of law enforcement agency was not satisfactory, as they could not help the victim SME in finding the attackers. This indicates that SMEs might find little or no help from outside if they are the victim of cybercrime. In addition, **SMEs do not believe that they are the target of cybercriminals.** SMEs reasoned out, as they are small business owners, the attackers cannot get financial gain by attacking them. This reasoning can be true, but still it is not preventing attackers from attacking SMEs. Moreover, the victim SMEs will never disclose their victimization incidents to lose reputation in the business and loose trust of their customers. So being cybercrime victim not only will make SMEs to interrupt business operations, but also it will cost them their companies' goodwill to the customers.

Expectations: Based on different literature reviews, this study has broken down its main research questions into four expectations. The first expectation was ***"An SME with fewer employees is less likely to have IT security measures and policies",*** which can be supported by the result of this study. The smaller number of surveyed samples indicates the use of IT security technology increases with the increasing number of employees. As well, the presence of documented policy is not common in SMEs with a small number of employees. Using proprietary IT solution software and well-documented ISO approved policy cost a lot of money for the company, and SME tend to reluctant to invest money in

those issues. This expectation aligns with Johnson and Koch's [50] statement "small SMEs would not pay for IT security".

The second expectation was ***"Most SMEs do not have policies for BYOD and Cloud Computing"***, which was constructed based on Dojkovski [61] [62] statement "SME owners do not have sufficient awareness of IT security". The study found that most SMEs do not have a policy for BYOD (Only 43% of the respondents has policy) supporting partial of second expectation. Also, 50% of the respondent SMEs have policy for Cloud Computing. Although 50% of the positive response does not provide any direction if the outcome of the study align with the first moment or not.

The third and the fourth expectations tried to identify which type of SMEs (IT or non-IT) are more vulnerable to cybercrime based on the cybercrime victimization incident. Nevertheless, this work could not collect much information about cybercrime victimization. It was not possible to reach a decision for both of the expectations, determining whether IT SME or non IT SME get victimized more often, hence determining their vulnerability to cybercrime.

Altogether the above discussion brings the answer to the main research questions the study posed in the beginning, "*What is the IT security practice of SMEs in Europe about security threats, focusing on BYOD and Cloud Computing?".* Although this survey could not identify the influencing factors based on employee's technical background due to lower sample size; in all the given case, the scenario is not well. SMEs with a small number of employees do not have a policy and pay less attention to IT security measures. BYOD and Cloud Computing are acceptable practices among SMEs, but still the SMEs do not follow or impose rules on SME to safely practice these trends. SME expects the employees to be self-aware of the security threats based on their IT backgrounds. This kind of expectation only shows SME's lack of interest in investing more time or money

on IT security. Finally, SMEs still do not believe they can be a target of cybercrime attack, as they do not get the news about SME being cybercrime victim that often. All the reasons give SMEs the false sense of security against cybercrime, and give them the reasons to be less concerned about it, hence making them vulnerable to cybercrime.

7. REFERENCE

Grey Studies

1. Enisa General Report 2012 Availble:http://www.enisa.europa.eu/publications/programmes-reports/general-report-2012; Last accessed: 2014/03/01

2. National White Collar Crime Center 2012. Internet Crime Report, Available:https://www.ic3.gov/media/annualreport/2012_IC3Report.pdf, Last Accessed: 2014/003/01

3. 2013 Norton Report, Available:http://www.yle.fi/tvuutiset/uutiset/upics/liitetiedostot/norton_raportti.pdf. Last Accessed: 2014/03/01

4. Unsecured economies: Protecting vital information, Available:http://www.cerias.purdue.edu/assets/pdf/mfe_unsec_econ_pr_rpt_fnl_online_012109.pdf. Last accessed: 2014/03/01

5. Hyman, P. 2013. Cybercrime: it's serious, but exactly how serious? Commun. ACM. 56, 3 (2013),18–20.

6. Kasperky Lab 2013. Kaspersky Global IT Security Risks Survey 2013. Available:http://media.kaspersky.com/en/businesssecurity/Kaspersky_Global_IT_Security_Risks_Survey_report_Eng_final.pdf. Last Accessed: 2014-03-01

7. CERT Australia 2012. Cyber Crime and Security Survey. Available:http://www.canberra.edu.au/cis/storage/Cyber%20Crime%20and%20Security%20Survey%20Report%202012.pdf; last accessed: 2014/03/10

8. CERT 2013 US State of Cybercrime Survey, Available:http://resources.sei.cmu.edu/asset_files/Presentation/2013_017_101_58739.pdf, Last Accessed:04/04/2014

9. 2013 Cost of Cyber Crime Study: Global Report. Available: http://www.hpenterprisesecurity.com/ponemon-2013-cost-of-cyber-crime-study-reports.Last Accessed: 2014/03/01

10.Top 10 Threats to SME Data Security. Available:https://www.watchguard.com/docs/whitepaper/wg_top10-summary_wp.pdf.Last Accessed: 04/04/2014

11.ISO/IEC 27005:2011 Information technology — Security techniques — Information security risk management (second edition), Int'l Org. Standardization, 2007. Available:http://www.iso27001security.com/html/27005.html. Last Accessed: 04/16/2014

12.ISO 27001 Security, Guideline for Information Asset Valuation
Available:http://www.iso27001security.com/ISO27k_Guideline_on_information_asset_valuation.pdf . Last Accessed: 04/16/2014

13.ISO/IEC 27005:2011 Information technology — Security techniques — Information security risk management (second edition), Int'l Org. Standardization, 2007.
Available:http://www.iso27001security.com/html/27005.html. Last Accessed: 04/16/2014

14.The Open Group. Technical standard risk taxonomy,
Available:http://pubs.opengroup.org/onlinepubs/9699919899/toc.pdf. Last Accessed: 04/16/2014

15.The NIST Definition of Cloud Computing,
Available:http://www.nist.gov/itl/cloud/upload/cloud-def-v15.pdf, Last accessed: 04/04/2014

16. Verizon Business RISK Team, "2008 Data Breach Investigations Report".
Available: www.verizonbusiness.com/resources/security/databreachreport.pdf. Last Access: 04/04/2014

17.A. Smith, "Mobile Access 2010," Pew Research Center, July 2010;
http://www.pewinternet.org/~/media/Files/Reports/2010/PIP_Mobile_Access_2010.pdf. Last Accessed: 04/16/2014.

18.A. Savvas, "European Firms Allow BYOD Despite Security Concerns," Computer World UK, 23 May 2012; Available:https://www.computerworlduk.com/news/mobile-wireless/3359491/european-firms-allow-byod-despite-security-concerns. Last Accessed: 04/16/2014

19."Cisco Study: IT Saying Yes to BYOD," Cisco, 16 May 2012;
Available:http://newsroom.cisco.com/release/854754/Cisco-Study-IT-Saying-Yes-To-BYOD. Last Accessed: 04/06/2014

20.Paul Ruggiero, J.F. 2011. Cyber Threats to Mobile Phones. Available:https://www.us-cert.gov/sites/default/files/publications/cyber_threats-to_mobile_phones.pdf Last Accessed:2014-03-20

21.ISBS (2006) Information Security Breaches Survey 2006, Department of Trade and Industry, UK.
Available:http://webarchive.nationalarchives.gov.uk/+/http://www.dti.gov.uk/files/file28343.pdf, Last Accessed: 04/04/2014

22.European Union Agency for Network and Information Security 2013. ENISA Threat Landscape. Available:http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/ENISA_Threat_Landscape/at_download/fullReport; Last Accessed: 2013-12-30

23.International Organization for Standardization 2012. ISO/IEC 27000:2012. International Organization for Standardization 2012. ISO/IEC 27000:2012.
Available:http://www.iso27001security.com/html/iso27000.html;Accessed: 2014-04-03

24.O'Halloran, J. (2003) ICT business management for SMEs, Computer Weekly, December 11.

25. Verizon Risk Team. (2013). The 2013 Data Breach Investigations Report: Verizon. Available: http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2013_en_xg.pdf. Last Accessed: 04/04/2014

26.Cloud Computing and SME's in UK, A report from the Cloud Stewardship Economics Project Group sponsored by Technology Strategy Board; Available: http://www.iisp.org/imis15//Cloud Computing_and_SME's_in_UK.pdf. Last accessed: 2014/03/03

27.Kristof K. (2010, IRS Policies Protect 1.2 Million Identity Thieves. Available: Available:http://www.cbsnews.com/8301-505144_162-36941966/irs-policies-protect-12-million-identity-thieves/. Last accessed: 04/16/2014

28.McCoy K. 2008, Identity thieves tax the system. Available:http://www.usatoday.com/money/perfi/taxes/2008-04-10-id-theft_N.htm. Last accessed: 04/16/2014

29.European Commission (2003-05-06). "Recommendation 2003/361/EC: SME Definition". Retrieved 2014-04-03

30."Europeans and their Languages" Available:http://ec.europa.eu/public_opinion/archives/ebs/ebs_243_en.pdf. Last accessed: 2014/03/03

31. 2014 Data Breach Investigations Report, Verizon. http://www.verizonenterprise.com/DBIR/2014/.#sthash.x7SaQWVv.dpuf. Last Accessed: 04/05/2014

32. B. Hoard, 8M cell phones will be lost in '07 – how to back yours up, Computerworld, Jul. 2007.

33. 2013 Cost of Cyber Crime Study: United Kingdom. http://www.hpenterprisesecurity.com/ponemon-2013-cost-of-cyber-crime-study-reports. Last Accessed: 04/04/2014

Peer Review:

34. Magklaras GB, Furnell SM. (2004) "The Insider Misuse Threat Survey: Investigating IT misuse from legitimate users" Available:http://folk.uio.no/georgios/papers/IWAR04MagklarasFurnell.pdf.Last Accessed:05/05/2014

35.Dimopoulos, V. et al. 2004. Approaches to IT Security in Small and Medium Enterprises. Australian Information Security Management Conference.

36.O'Regan N. and A. Ghobadian, "Testing the homogeneity of SMEs: The impact of size on managerial and organisational processes," European Business Review, vol. 16, pp. 64-77, 2004.

37.The new SME definition: User guide and model declaration, Available:http://ec.europa.eu/enterprise/policies/sme/files/sme_definition/sme_user_guide_en.pdf Last Accessed: 04/04/2014

38.Dimopoulos, V., Furnell, S.M., Jennex, M. & Kritharas, I. (2004) Approaches to IT Security in Small and Medium Enterprises, in Proceedings of the 2nd Australian Information Security Management Conference 2004, Perth, Australia.

39.Gupta, A. & Hammond, R. (2005) Information systems security issues and decisions for small businesses, Information Management & Computer Security, 13(4), 297-310

40.Helokunnas, T. & Iivonen, I. (2003) Information Security Culture in Small and Medium Size Enterprises, Seminar Presentation, Institute of Business Information Management, Tampere University of Technology, Finland

41. Furnell, S.M., Gennatou, M. & Dowland, P.S. (2000) Promoting Security Awareness and Training within Small Organisations, in Proceedings of the 1st Australian Information Security Management Workshop, Deakin University, Geelong, Australia

42. Johnson, D.W. & Koch, H. (2006) Computer Security Risks in the Internet Era: Are Small Business Owners Aware and Proactive? In Proceedings of the 39th Annual Hawaii International Conference on System Sciences (HICSS'06), IEEE Society Press.

43. Kelly, B.B. (2012). Investing in a centralized cybersecurity infrastructure: Why "hacktivism" can and should influence cybersecurity reform. Boston University Law Review. 92, 5 (2012), 1663–1711

44. Doherty, N.F. & Fulford, H. (2006) Aligning the Information Security Policy with the Strategic Information Systems Plan, Computers & Security, 25(2), 55-63.

45. Suchan, W. and Sobiesk, E. (2006). Strengthening the weakest link in digital protection. IEEE Security and Privacy. 4, 6 (2006), 78–80.

46. Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., ... & Zaharia, M. (2010). A view of cloud computing. *Communications of the ACM*,*53*(4), 50-58.

47. Dhillon, G. & Backhouse, J. (2001) Current Directions in Information Systems Security Research: Toward Socio-Organizational Perspectives, Information Systems Journal, 11(2), 127-153

48. Sánchez, L.E. et al. (2010). Managing the asset risk of SMEs. (Krakow, 2010), 422–429

49. Neumann, P. G. 1999. "Risks of Insiders," Communications of the ACM (42:12), pp. 160.

50. Durgin, M. (2007). "Understanding the Importance of and Implementing Internal Security Measures," SANS Institute Read Room.

Available:https://www2.sans.org/reading_room/whitepapers/policyissues/1901.php. Last Accessed :04/16/2014

51. Lee, J., and Lee, Y. (2002). "A Holistic Model of Computer Abuse within Organizations," Information Management and Computer Security (10:2/3), pp. 57-63.

52. Gordon, L. A., Loeb, M. P., Lucyshyn, W., and Richardson, R. (2006). "CSI/FBI Computer Crime and Security Survey," Computer Security Institute (available online at Available:http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2006.pdf. Last Accessed: 04/04/2014

53. Besnard, D. & Arief, B. (2004) Computer Security Impaired by Legitimate Users, Computers & Security, Vol: 23, page 253-264.

54. Azarnik, A.; Shayan, J.; Alizadeh, M.; Karamizadeh, S., (2012). "Associated Risks of Cloud Computing for SMEs"; Open International Journal of Informatics (OIJI), VOL 1; Page 37-45.

55. Aron R., E. K. Clemons, and S. Reddi, (2005), "Just Right Outsourcing: Understanding and Managing Risk," in System Sciences, 2005. HICSS '05. Proceedings of the 38th Annual Hawaii International Conference on, pp. 214-214

56. Chen Y. and A. Bharadwaj, (2009) "An Empirical Analysis of Contract Structures in IT Outsourcing," Info. Sys. Research, vol. 20, pp. 484-506.

57. Clemons E. K. and L. M. Hitt, (2004) "Poaching and the Misappropriation of Information: Transaction Risks of Information Exchange," J. Manage. Inf. Syst., vol. 21, pp. 87-107.

58. Walden E. A., (2005) "Intellectual property rights and cannibalization in information technology outsourcing contracts," MIS Q., vol. 29, pp. 699-720.

59. Cheng, L. et al. (2013). Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory. Computers and Security.

60. Sikkel, D. (2009). Opzet enquête financieel-economische criminaliteit en computercriminaliteit. Leidschendam, Nl.: Sixtat, WODC.
Available:http://www.wodc.nl/images/opzet-enquete_tcm44-301432.pdf. Last accessed: 2014/03/03

61. Dojkovski, S.; Lichtenstein, Sharman; and Warren, Matthew J., 2007) "Fostering Information Security Culture in Small and Medium Size Enterprises: An Interpretive Study in Australia" (ECIS 2007 Proceedings. Paper 120.

62. Dojkovski, S.; Lichtenstein, Sharman; and Warren, Matthew J., (2006) "Challenges in Fostering Information Security Culture in Small and Medium Size Enterprises", in preceding of 5th European Conference on Information Warfare and Security, 1-2 June, 2006. National Defense College, Helsinki, Finland.

63. Han Y.,"Cloud Computing: Case Studies and Total Costs of Ownership" Information Technology and Libraries. December 2011. Volume 30, No 4;
Available:http://ejournals.bc.edu/ojs/index.php/ital/article/view/1871/1709, Last Accessed: 8/5/2014

64. Xinhui Li , Ying Li , Tiancheng Liu , Jie Qiu , Fengchun Wang, (2009) The Method and Tool of Cost Analysis for Cloud Computing, Proceedings of the 2009 IEEE International Conference on Cloud Computing, p.93-100, September 21-25.

65. Ambrož Milan."Security Culture Impact on Security Excellence in a Company". Innovative Issues and Approaches in Social Sciences, vol.5, no.1:70-87, DOI:http://dx.doi.org/10.12959/issn.1855-0541.IIASS-2012-no1-art06

66. Yan, G., Chen, G., Eidenbenz, S., & Li, N. (2011, March). Malware propagation in online social networks: nature, dynamics, and defense implications. In *Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security* (pp. 196-206). ACM.

67. Cox, A., Connolly, S., and Currall, J. (2001). Raising information security awareness in the academic setting. VINE , 11-16

68. Moshchuk, A., Bragin, T., Gribble, S. D., & Levy, H. M. (2006, February). A Crawler-based Study of Spyware in the Web. In *NDSS*.

69.Kaur, J.; Mustafa, N., (2013) "Examining the effects of knowledge, attitude and behavior on information security awareness: A case on SME," Research and Innovation in Information Systems (ICRIIS), International Conference on , vol., no., pp.286,290, 27-28 Nov. 2013.

8. APPENDIX

Questionnaire:

The full version of the questionnaire is available in this like as a google questionnaire form:

https://docs.google.com/forms/d/1MOdr0tZOtY-OOv8snxJ-wD4hIpScCAjXPJLLDbyNgdY/viewform

Question 18: Over the last 12 month period (2013-2014), which of the following technologies are being used in your company for IT security purposes?

Result:

	Total	R1	R2	R3	R4	R5	R6	R7	R8	R9	R10	R11	R12	R13	R14	R15	R16
Anti-virus/-malware protection	13		1	1	1	1	1	1	1	1	1	1	1			1	1
Firewalls	13	1	1	1	1	1	1	1	1	1	1	1				1	1
Anti-spam/-phishing tools	10		1		1	1	1	1	1	1	1	1				1	
Virtual Private Networks (VPN)	10	1	1		1	1	1	1	1	1	1	1					
Encrypted login/sessions (SSL/HTTPS)	10	1	1	1	1	1		1	1	1	1				1		
Intrusion detection systems	7	1	1		1		1	1			1		1				
Encrypted files	7	1	1		1		1	1		1	1						
Use of legal software	8		1		1		1	1		1	1	1	1				
Access control (Biometrics/tokens/authenticators)	5		1		1			1		1	1						
Uninterrupted power supply (UPS) for servers	6	1	1					1		1	1	1					
Physical theft prevention (Kensington locks)	3		1					1			1						
Offsite backups	5		1	1				1				1	1				
Don't know	1													1			
Other	2	2															

Question 16: Which Cybersecurity policies in your company are in place at the moment?

Result:

	Total	R1	R2	R3	R4	R5	R6	R7	R8	R9	R10	R11	R12	R13	R14	R15	R16
Business continuity plan for IT	5		1				1	1		1	1						
Hired an external company for computer security	3		1							1			1				
Periodic vulnerability / risk assessment of IT	5	1	1				1		1		1						
Hired a computer / network monitoring center	4		1		1						1	1					
Have formal/documented computer security standards	7	1	1	1	1				1	1	1						
Training of personnel in security procedures	7	1	1	1			1	1		1	1						
Keeping media backup	11	1	1	1	1		1	1	1	1	1	1	1				
Control against the pirated software	8			1	1		1	1	1	1		1				1	
Management of removable computer media (i.e: USB sticks)	5	1	1					1		1	1						
Safety measures for using personal devices for work	7				1		1			1	1	1				1	1
Cloud computing security measures	8		1		1		1		1	1	1		1		1		
Don't know	2					1								1			
None of the above	1					1											
Other:	4		disas		Lapto			remot			data s						

Question 38: Over the last 12 month-period (2013-2014), which of these IT security related incidents has your company faced so far?

Result:

	Total	R1	R2	R3	R4	R5	R6	R7	R8	R9	R10	R11	R12	R13	R14	R15	R16
Virus/malware attack/infection	4							1	1							1	1
Spam/phishing	2								1								1
Hacker intrusion	1							1									
Unauthorized access of sensitive data/system by outsider	1							1									
Data loss	0																
Theft of electronic device	0																
Computer facilitated financial fraud	0																
Denial of service attack	0																
Unauthorised privileged access	0																
Degradation of network	0																
System penetration	0																
Web site defacement	1							1									
Theft of customer information	0																
None of the above	2	1											1				
Other	1						botnets							I don't	1		