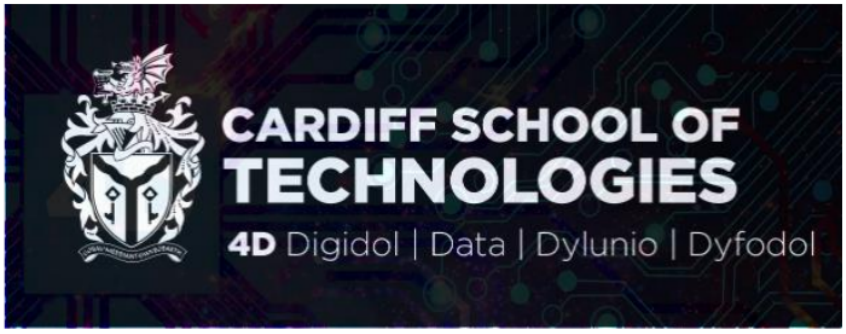
# st20219772 CIS7028 WRIT1.docx

*by* Vyshnavi Muthumula

**Submission date:** 12-May-2022 11:48PM (UTC+0100)
**Submission ID:** 179806563
**File name:** 104532_Vyshnavi_Muthumula_st20219772_CIS7028_WRIT1_1250544_666051190.docx (292.12K)
**Word count:** 3904
**Character count:** 22056




| |
|---|
| **Cardiff Metropolitan University** |
| **Cardiff School of Technologies** |
| |
| **Academic Year: 2021/2022** |
| **Term: 2** |
| **Module Name:** Information Security |
| **Module Code:**CIS7028 |
| **Module Leader: Dr Liqaa Nawaf** |
| **MSc Programme:** |
| |
| **Assignment Title: Samsung Cyber attack** |

| | |
|---|---|
| **Student Name: Vyshnavi Muthumula** | **Student ID: 20219772** |
| **Data Submitted:** | **Mark:** |
| **Feedback:** | |
| **Signature:** | **Date:** |

# Contents

## Introduction

Cyber security refers to the protection of data from unauthorised people (Hackers) across different server networks and from attacks.

**Why cyber security is important?**

Cyber security helps users in protecting their data against concerns such as data leakage, hardware or software damage, or electronic data loss. It will be extremely beneficial to both corporations and people. If user fails to protect the data, all of their clients' personal and sensitive information will fall into the wrong hands, causing complications. As a result, cyber security is critical, and everyone in the corporation is responsible for data security.

https://www.futurelearn.com/info/blog/how-to-deal-with-cyber-security-threats

**About Samsung:**

Samsung began as a tiny business selling dried fish and noodles in 1938. Later some year's it started moving to build electronic devices like smart mobiles, television and electronic chips for designing the devices like Robots, aeroplane and other electronic devices.

Samsung established in 13 January 1969 founded by Suwon-si, South Korea. The stock price of the Samsung is US$1,284.50. It employs over 290,000 people and has sales networks in 74 countries. Out of all electronic devices Samsung Galaxy is the popular one than the original one Samsung solstice.

https://en.wikipedia.org/wiki/Samsung_Electronics

In recent devices Samsung is one of the largest electronic manufacture companies. (https://www.nature.com/articles/s41928-020-0418-8)

## Task 1

**Current Risks post COVID19 Pandemic**

Risk is a combination of threats and vulnerabilities which intimates the company for reducing damage. There are different types of risks present such as risk from employees, third party tools effect, security issues and sudden collapse of data because of server down.

## Task 1.1

Biju, J.M., Gopal, N. and Prakash, A.J., 2019. Cyber attacks and its different types. *International Research Journal of Engineering and Technology*, *6*(3), pp.4849-4852.

Cyber assaults are the process of launching targeted attacks on web data in order to damage or steal it. A hacker can be an individual or a group of individuals. Data is now stored in systems or computers.

Capturing the data, saving, and using the data which contains sensitive information is very difficult. There are many risks which affect the product loss.

There are different types of cyber risks present, some are listed below.

**Phishing:** Phishing is an attack of getting fraudulent emails or text messages from a people for grabbing sensitive information like username, password, financial details such as credit / debit card details. It practically seems that the email is from a reputable source, but it isn't. Many people have acclimated to work from home as a result of COVID19, and they are constantly checking for mail. As a result of recent incidents, majority of people are using social media to check job profiles, etc. The user must keep note of the following key points.

1. Verify whether the sender details looks correct or not.

2. Just check the links before clicking it.

3. Check the subject line.

4. Read all the body of the mail has any grammatical issues or not.

5. Check headers of the mail and regards.

**Ransomware attack:** Ransomware is a type of malware that encrypts or prevents user to access the files. After that the attacker demands money for decrypting the data so that victim can re-access their files. The attack may happen by emails or links so that user can click on it and the can inject the malware into their system.

**MITM:** A man-in-the-middle attack is when an attacker establishes a connection between sender and receptor so that he can modify the message. This alter can be done without knowing by sender or receiver.

**DDos:** A Denial of Service/Distributed Denial of Service Attack (DDos) occurs when a hacker uses multiple devices and used them to overload the target systems. They make the site slow for sometime so that user won't be able to access the data.

**Password attack:** It is a technique used to grab the user password by some decryption techniques. Keeping weak password is the biggest vulnerability for the company because hacker can easily hack it.

**SQL Injection Attack:** Retrieving data from database by injecting some SQL queries. SQL injection is the **highest risk** for the organization because they can delete or stole or update it.

In 2020 Samsung attacked by data breach because of this data breach 150 users personal details are leaked.

How this attack happened:
One strange notification popped into the thousands of Samsung users mobile via Find My Mobile app and the message contains '1'.

Because of this push message some users change their password for safer side. As soon as they find the issue they immediately blocked the user to change their passwords or access sites because while they trying to change the password they are required to enter their old sensitive details this is what hackers want. That's why Samsung team removed the access to login to the store until the issue is fixed.

**Samsung cyber attack in 2021**

In 2021 found Samsung pre installed apps are allowed hackers to steal the victims data, messages, videos, call records and contacts.

A mobile security firm discovered flaws in the Samsung Secure Folder app that could be used to steal contact information, and in Samsung Knox security software that could be used to install malicious apps. Samsung fixed the vulnerabilities.

## Task 1.2

### Alternative standards for protecting data from attacks:

There are many ways to protect the data from hackers as listed below.

1. Educating the employees: Pandemic caused several issues to organization because of work from home. Employees working from home and using public WIFI which leads for data leak. (https://www.sciencedirect.com/science/article/pii/S2214785321029345?casa_token=QJ51H8us-LEAAAAA:AGEZUmVpGdQDNyalJnNs5DRgXzd5Glyqb01hh3umfblwBPfP1dLrRL2KD3s0a4TzaeyER5LfEg) Organisation must educate their employees regarding cyber issues. Like providing **VPN** creates a secure environment between employee and server. Employees must avoid using public WIFI.

2. Security policies: Every application has their own security features. While additional precautions are still necessary based on new trends and risks, organization vendors are familiar with their own products and for providing secure environment for clients they always invest money one special resources.

3. Secure hardware: Every organization contains hardware as well as software. Cyber attack will happen if the hardware stolen because hardware contains chips and hard discs which have all important data.

4. Creating backups: Encrypt the sensitive information such as employee details and customer data by keeping it secure in a safe environment such as creating backups.

5. Purchase cyber-security insurance: Investing money in insurance is very good plan because, if there is any loss after cyber attack person can claim for their loss.

6. Secure Password: Send a notification to employee saying that password needs to update for every 14 days so that chances of getting data breach will be less.

7. Limit network administrator access: In **Mccumber cube** Authentication is one of the important factors for securing the data. Authenticate the people who access the data over the network. Admin access should be limited to some people otherwise chances for data breach are more.

8. Anti-malware and firewall software should be used: Firewalls are used to pass the data from customer to server easily without traffic. It is also used for protecting the data from hackers and Trojans.(https://www.entrepreneur.com/article/316886)

9. By using machine learning algorithms organizations can detect the cyber attacks and it has the ability to defend the malware attacks and botnet behaviour. ( Delplace, A., Hermoso, S. and Anandita, K., 2020. Cyber Attack Detection thanks to Machine Learning Algorithms. *arXiv preprint arXiv:2001.06309*.)

10. Protecting from Free WIFI: Samsung uses **Secure WIFI** for protecting data from free wifi. It encrypts the data which is going from traffics and gives a secure way for customer and server.

"The types of vulnerabilities AbstractEmu takes advantage of also point to a goal of targeting as many users as possible, as very contemporary vulnerabilities from 2019 and 2020 are leveraged," they explained."One of the exploits used CVE-2020-0041, a vulnerability not previously seen exploited in the wild by Android apps. Another exploit targeted CVE-2020-0069, a vulnerability found in MediaTek chips used by dozens of smart phone manufacturers that have collectively sold millions of devices. As a hint to the threat actor's technical abilities, they also modified publicly available exploit code for CVE-2019-2215 and CVE-2020-0041 in order to add support for more targets."

## Task 1.3

**General Data Protection Regulation and International Organization for Standardisation (ISO 27001):**

**General Data Protection Regulation 2016/679 (GDPR):** It is a regulation which used to protect the data in Europe. Along with protection it also maintains the privacy. There are 7 principles in GDPR. They are Lawfulness, fairness and transparency, Purpose limitation, Data minimization, Accuracy, Storage Limitation, Integrity and confidentiality, Accountability.

Lawfulness, fairness and transparency: Samsung is following GDPR rules. According to this principle Samsung is loyal to their customers (as well as employees), must be clear and

honest with customer about why they are collecting their personal data and how they plan to use it.

GDPR imposes new security and data protection obligations on businesses (2018). Samsung build **Samsung Knox** in devices to protect mobile information and allows customer to operate whenever they need. The main purpose of designing this Samsung Knox is to keep personal and business data separately in different encrypted repositories and it also enables remote work management. The business data can be operated by business people in work space container and personal data like photos and messages will be stay safe (private). French Agence Nationale de la Sécurité Des Systèmes D'information (ANSSI) given some points to secure the data. Samsung segregated those into 7 principles those are listed below.

**Control from centre:** A mobile security policy should include device management and user profile management from a central location. Enterprise Mobility Management (EMM) should be considered in addition to Mobile Device Management (MDM). Not only focus on hardware security, check what device user has and study it and then understand the sensitivity of the data.

**Drive authorisations:** For security purpose segmentation is important like user profiles according to their positions they can have access. With GDPR the users who are handling sensitive data must be careful. Samsung Knox takes care of it.

**Control access:** Restricting the number of attempts to change the password. Knox Manage allows user to manage password rules in a fully customizable way.

**Ensure Operating System integrity:** Updating the OS leads to less attacks and vulnerabilities. Samsung has some services like Knox configure, manage and workspace. These are always checks the **integrity** of the operating system and any updates coming from unauthorized server it will block.

**Apps and Data secure:** While downloading any application from app store user must need to verify once whether it's a secured one or not. Knox workspace divides applications into "blacklist" and "whitelist" categories.

**Personal and Professional data segregation:** Samsung Knox segregating the data into two parts such personal and professional so that user sensitive information will be in safe container. The entire will be in encrypted format.

**Securing data remotely:** If mobile are stolen or get lost, retrieving data will be difficult for organizations. Knox configures enables remote accessing for locking the devices and will delete data if it is necessary. Geo-location of the data also recovered by using Knox configures.

**ISO 27001 certification** helps organizations to protect, maintain, establish, and improve data. Samsung also received certification from **British Standards Institution** (BSI) which is recognized by ISO 27001.

## Policies and McCumber cube:

The goal of the company is to protect consumer's data. Samsung also have some set of rules for protecting consumer data. The guidelines or laws which Samsung has will vary depending

on country. Samsung is providing training to their employees in these area. **Data Protection Handbook, Privacy Policy on Data sharing with Third Party people.** These third parties use cookies, beacons, tracking pixels, and other tools to collect the information.

Samsung is following 3 key principles to protect customer personal data. They are choice, Transparency and security.

**Choice:** Samsung main motivation is to satisfy customers and allows consumers to make choices on the use of their personal data. Therefore, it let users to decide how their data to be handled while using products and services.

**Transparency:** Usually organizations take personal information for security purposes like if user account was exposed then for retrieving user account, system needs to have some personal information that given by user, but the hacker won't be able to know those sensitive data until unless they decrypt it. For providing better customized experience they need what consumer likes.

**Security:** By using strong data encryption techniques Samsung is protecting consumer data. For example in recent mobiles user notice so many new features popped up for securing the data like biometrics and face recognition technology.

Data shared by Samsung:

1. Affiliates: Other Samsung Electronics group companies which they control or own.
2. Business Partners: The partners which they connected.
3. Service Providers: Companies that provides services for or on behalf can also have consumer's personal data. They provide services like advertising the product, taking consumer satisfaction surveys, billings, third-party websites and sending emails if needed on behalf of the organization.
4. Law protection: For legal purposes Samsung need to send their consumer's data to Government if there is any criminal issues happened.

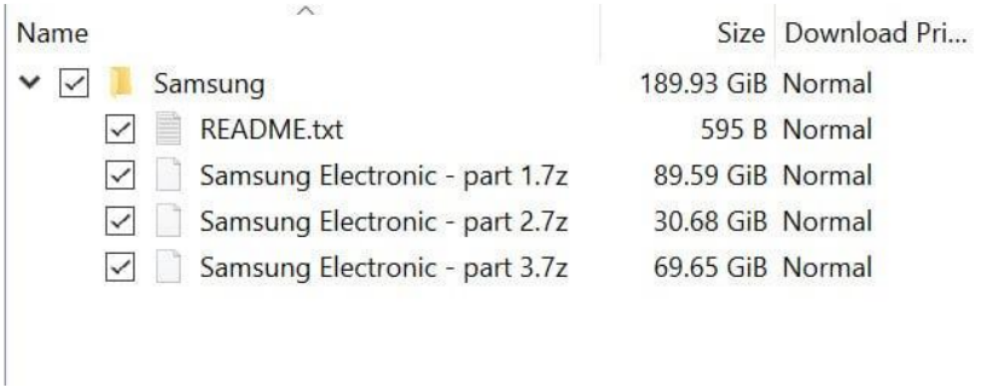
# Task 2

## Task 2.1

**Samsung data breach happened on March 7, 2022**

During COVID period most of the companies prefer work from home and employees are most vulnerability to the hackers because of public environment. The place where employees work is not protected as office environment and employee won't be able to get the proper security measures, software updates, key policy rules, VPN access because of less secure WIFI, this is reason Samsung had attacked even after following security measure. Hackers injected some torrent files to telegram and 400 people downloaded it which resulted into attack.

https://www.techradar.com/uk/news/samsung-hacked-galaxy-phones-leaked




Based on reports (as shown in above picture) the leaked data is divided into three parts.

1. First part contains source code copy and imported applications data such as security, Defence, Knox, TrustApps or Bootloaders.
2. Second part contains security and encryption related data present.
3. Third part contains Data repositories which have front end, backend, defence engineering data along with SES (Bixby, Smart things and store. https://www.bleepingcomputer.com/news/security/hackers-leak-190gb-of-alleged-samsung-data-source-code/

**Loss and vulnerabilities:**

Samsung source code was leaked and posted in Telegram. Lapsus$ reported over 190 GB data steeled by hackers which includes confidential data like source code of Galaxy smart phones. This source code includes

1. Samsung biometric authentication algorithms
2. Bootloader code
3. Biometric unlock operations machine learning algorithms
4. Samsung connected with Qualcomm (chip maker) for HW-chassis which supports Exynos modem because of this attack Qualcomm source code also leaked.
5. Activation server details
6. Technologies used for authorizing and authenticating the Samsung accounts also under part of source code which includes APIs and server calls.

The issue was resolved quickly when it was noticed and no customer data as leaked according to Samsung. Lapsus$ did not end there, with allegations that biometric unlock algorithms, bootloader source code, and Samsung activation server code was also included in the leak. Even though customer data didn't leak, company had lots of issue because of this attack, as source code of Galaxy mobiles was leak it had chances of getting copied by other companies.

The leaked data was divided into three compressed files of 190GB, which Lapsus$ posted to a torrent that appears to be quite popular, with over 400 peers spreading the content. Confidential data leak content will spread rapidly.

The vulnerability for this attack is TrustZone Operating System (TZOS), which is part of the security-sensitive Trusted Execution Environment (TEE) of Galaxy devices, which has weaknesses in its cryptographic design and code structure. Researchers are saying source code for Trustzone operating system was also leaked.

The reason for this entire attack is Nvidia vulnerabilities. Samsung uses RTX 30-series graph card which designed by Nvidia. Nearly 1TB of sensitive data, including over 71,000 employee passwords and proprietary source code, was stolen from NVIDIA's networks in February 2022. Lapsum group blackmail Nvidia to remove the Lite Hash Rate (LHR) from RTX 30 series graphic card, but Nvidia didn't remove it that is the reason for Samsung data breach. When mining Ethereum and other crypto currencies, the Lite Hash Rate is used for limiting the graphic cards' performance.

Zhu, Y., Cheng, Y., Zhou, H. and Lu, Y., 2021. Hermes attack: Steal {DNN} models with lossless inference accuracy. In *30th USENIX Security Symposium (USENIX Security 21)*.

Samsung claimed responsibility on Telegram, Message services which encrypts and third party providers (Nvidia). https://www.rcrwireless.com/20220309/telco-cloud/samsung-confirms-ransomware-attack

## Task 2.2

**Attack Illustration:**

This attack is one of the major attack for Samsung Electronics company due to this attack Samsung faced security issues and reputation damage. The main reason for this security breach is of Samsung vulnerabilities. Samsung Electronics are not a alone complete package, it is tie-up with Qualcomm for processers, chips, RF systems and Nvidia (Software provided company) for graphic cards. So if Nvidia products or Qualcomm products hacked then automatically Samsung affecting to resolve those issues Samsung or any company needs to be aware of vulnerabilities for that product before using them. The reason for Samsung security breach is vulnerability in the products mainly in the RTX 30 series graphic card which designed by Nvidia. In the initial stage of attack Samsung confirms that the attack happened but it is not affecting any customer or employee sensitive data. This attack is doesn't cause greater loss to company on production sales wise but they lost some important source code and now again they need to re-modify their source code because of security breach. This attack was done y Lapsus$ group. The source code for each Trusted Applet (TA) installed in Samsung's TrustZone environment for sensitive operations is one of the data Lapsus$ claims. Other sources of data Lapsus$ claimed include the biometric unlock algorithms, all recent Samsung devices bootloader code, Qualcomm's confidential source code, Samsung's activation server code, and the complete APIs and services used for authorizing and authenticating Samsung accounts. Total of 198 GB source code data leaked on Telegram by Lapsus$ group. The aim of this group, along with others, is to steal sensitive either business or employee or customer data, spread threats, and extort victims. This group hacked so many companies like Microsoft, Globant, Okta along with Nvidia and Samsung.

**Vulnerability tools:**

There are several ways for hacking and each minor point also they will consider. One way is to target employee or customers like they may send survey link to the people which has questions like DOB, maiden name, favourite colour or place and so on,. Based on these answers hackers try to guess the passwords.

Today web-applications are some of the most widely used applications. They are user-friendly, very responsive, dynamic structure and well structured. Web application integration for APIs or services is very easy and which connects any applications with database very easily. This makes attackers to think about it more before hacking any web application, if they hack correctly all the sensitive information will be in trouble. Ensure that any remote administration tools and services used by the organization are strictly controlled, and disable the unused tools. Whenever if new remote access software installs without admin permission then **Endpoint Detection and Response (EDR) and Extended Detection and Response (XDR) platforms recognises** them and blocks them to not install in the device. Lapsus observed that Remote desktop protocols (RDP) allow user to enable and access the sessions when they needed, this is proven while doing simulations for breaches. If desktops, laptops, servers, and cloud instances are wrongly configured or powered on by a hostile assault, it is also feasible to gain access to them.

Hackers use these tools to exploit vulnerabilities.

They are BurpSuite, Commix, w3af, Jexboss and OASP ZAP.

**MobSF:** This is an automated software scanner that runs under Kali Linux. It examines the code and generates a report which contains exploitable vulnerabilities in the mobile application.

**Nmap:** This tool used to find the vulnerabilities in the network and also identifies the target host. Also detects the issues in remote hosts.

(https://www.mygreatlearning.com/blog/ethical-hacking-tools/)

**BurpSuite:** It is a web proxy in Kali Linux server which allows hackers to stop the interaction between customer computer and server by introducing more traffic. By using this proxy they can change the submitted values by users and they can modify the original content. The chances for including malicious letters to the entries for collapsing web application are more.

**Commix:** Hackers can use this tool for exploiting the vulnerabilities which runs through command injection. Entire operating system data can be dragged with this tool by using terminal execution.

**Runtime Mobile security (RMS):** It is another tool which used to control the Android and IOS apps while they're are running. RMS can impute related methods, functions, arguments into the main source code and then they can modify everything (customer scripts).

https://resources.infosecinstitute.com/topic/top-18-tools-for-vulnerability-exploitation-in-kali-linux/

## Recommendations:

Make sure that any ***third-party tools*** that a corporation uses are thoroughly tested to see whether any issues or attacks will arise in the future.

Srinivas, J., Das, A.K. and Kumar, N., 2019. Government regulations in cyber security: Framework, standards and recommendations. *Future Generation Computer Systems*, *92*, pp.178-188.

Design ***firewalls*** for security purposes and the use firewalls is to allow only authorized people to the network (traffic). There are various types of fires are used for various security purposes. ***Encrypting*** the data is another key for vulnerability. All the important sensitive data is present in repositories if data is not encrypted then the chances for stealing data is very for hackers. So the information must be encrypted using any of the techniques like ***Symmetric key encryption, Advanced encryption Standard (AES) or Public key Encryption mechanisms*** then only user can decrypt it. Due to COVID19 majority of the companies prefers for work from home which leads employee to use his on wifi, it shows vulnerability to hackers. Although Software team providing awareness towards it, the attacks are occurring. Employee must needs to be responsible it. Consumer needs to update the mobile device up-to-date otherwise the new patches added for resolving the old flaws won't be solved and with leads back-door to hackers.

## References


Chowdhury, A., 2016, October. Recent cyber security attacks and their mitigation approaches–an overview. In *International conference on applications and techniques in information security* (pp. 54-65). Springer, Singapore.

Bordoff, S., Chen, Q. and Yan, Z., 2017. Cyber attacks, contributing factors, and tackling strategies: the current status of the science of cybersecurity. *International Journal of Cyber Behavior, Psychology and Learning (IJCBPL)*, *7*(4), pp.68-82.

Srinivas, J., Das, A.K. and Kumar, N., 2019. Government regulations in cyber security: Framework, standards and recommendations. *Future Generation Computer Systems*, *92*, pp.178-188.

Radanliev, P., De Roure, D., Page, K., Nurse, J.R., Mantilla Montalvo, R., Santos, O., Maddox, L.T. and Burnap, P., 2020. Cyber risk at the edge: current and future trends on cyber risk analytics and artificial intelligence in the industrial internet of things and industry 4.0 supply chains. *Cybersecurity*, *3*(1), pp.1-21.

Gouda, M.G. and Liu, A.X., 2007. Structured firewall design. *Computer networks*, *51*(4), pp.1106-1120.

Salam, A., 2020. Internet of things for sustainability: perspectives in privacy, cybersecurity, and future trends. In *Internet of Things for sustainable community development* (pp. 299-327). Springer, Cham.

# st20219772 CIS7028 WRIT1.docx

ORIGINALITY REPORT

| 19% | 16% | 3% | 11% |
|---|---|---|---|
| SIMILARITY INDEX | INTERNET SOURCES | PUBLICATIONS | STUDENT PAPERS |

PRIMARY SOURCES

| | | |
|---|---|---|
| 1 | www.helpnetsecurity.com<br>Internet Source | 3% |
| 2 | Submitted to University of Wales Institute, Cardiff<br>Student Paper | 2% |
| 3 | Submitted to University of Northumbria at Newcastle<br>Student Paper | 1% |
| 4 | jsju.org<br>Internet Source | 1% |
| 5 | Submitted to Middlesex University<br>Student Paper | 1% |
| 6 | www.samsung.com<br>Internet Source | 1% |
| 7 | www.SamSung.com<br>Internet Source | 1% |
| 8 | www.forbes.com<br>Internet Source | 1% |
| 9 | www.futurelearn.com | |

| | | |
|---|---|---|
| | Internet Source | 1% |
| 10 | Submitted to University of Maryland, University College<br>Student Paper | 1% |
| 11 | doras.dcu.ie<br>Internet Source | 1% |
| 12 | Submitted to The Robert Gordon University<br>Student Paper | 1% |
| 13 | Submitted to ICL Education Group<br>Student Paper | 1% |
| 14 | www.androidheadlines.com<br>Internet Source | 1% |
| 15 | Submitted to University of Bedfordshire<br>Student Paper | 1% |
| 16 | mafiadoc.com<br>Internet Source | 1% |
| 17 | news.livedoor.com<br>Internet Source | <1% |
| 18 | Submitted to University of Glamorgan<br>Student Paper | <1% |
| 19 | Submitted to Asia Pacific University College of Technology and Innovation (UCTI)<br>Student Paper | <1% |

| | | |
|---|---|---|
| 20 | Submitted to Croydon College<br>Student Paper | <1% |
| 21 | Submitted to University of Sunderland<br>Student Paper | <1% |
| 22 | www.schneier.com<br>Internet Source | <1% |
| 23 | www.securityweek.com<br>Internet Source | <1% |
| 24 | staging.aha.org<br>Internet Source | <1% |
| 25 | www.researchpublish.com<br>Internet Source | <1% |
| 26 | blogs.bournemouth.ac.uk<br>Internet Source | <1% |
| 27 | aes.safehouseencryption.com<br>Internet Source | <1% |
| 28 | akit.cyber.ee<br>Internet Source | <1% |
| 29 | analyticsindiamag.com<br>Internet Source | <1% |

| | | | |
|---|---|---|---|
| Exclude quotes | Off | Exclude matches | Off |
| Exclude bibliography | Off | | |