ISM COURSEWORK

Name: Nithesh Koneswaran
URN: 6474079
Username: nk00374

Appendix | Assets and Classification

Risk	Asset	Type	Category	Asset Value	Reason	CIA	Threat	Vulnerability	Ease of Exploitation	Likelihood of threat occurrence	Risk Scores from Table E.1	Business Impact	Impact LHM
R1	Wireless Access Points [1]	Real	Hardware, Network	2	Can be point of entry for an unauthorised entity to sensitive or confidential information that may impede GDPR if unprotected [1]	I, A	Individuals actively searching for unsecured wireless access points (wardriving) to gain unauthorised access the network and potentially steal sensitive data [2]	Having an unsecured wireless access point	L	L	2	Expect financial losses for the company and customers if data has been stolen. Damages to the company's reputation if the attack was the result of an unsecured WAP which could easily be protected. The company must pay a hefty penalty following the breach due to impeding GDPR.[4][6] Customers will also be needed to be compensated and appropriate response efforts will have to be made to alleviate the damages	M
R2	TalkTalk DNS Servers	Real	Hardware, Data, Network	3	The performance of the DNS server can affect customer satisfaction, if the server goes down frequently or for a long period of time, it will undoubtedly negatively affect TalkTalk's reputation.	I,A	Deliberate DDoS attack on TalkTalk's DNS Servers involving hundreds or thousands of customers	DNS servers can be prone to DDoS	M	L	4	Damages to company's reputation as customer's will be unsatisfied with the services TalkTalk provides. There is potential to lose existing customers to competitors. Engineers will be required to monitor and review the incident. Response efforts may be required to compensate affected customers.	M
R3	Miscellaneous USB devices [1]	Real	Hardware	1	Such devices could contain personal information or be compromised and repurposed to steal sensitive data. [1]	I,A	The Trojan human', the attacker could deliberately infiltrate the company disguised as an employee and infect the network via any means or steal equipment belonging to the company	Employees are prone to social conditioning. An employee might inadvertently or intentionally allow an unauthorised individual into a restricted area without realising.	M	L	2	Putting employees at risk, ensure security is tight to prevent unauthorised access. Stolen property and a data breach can put the company at a financial loss. Consequences of a security/data breach could impact the company's reputation.	M
R4	TalkTalk Offices	Real	N/A	2	Offices can hold sensitive information on paper copies so there is a potential for data to be leaked. Furthermore offices provide a working environment for TalkTalk employees.	C,A					3		M
R5	Business Team Employees	Real	People	1	TalkTalk's Business team is responsible in providing valuable services and products to business customers. The team's performance can affect the TalkTalk's image since it is linked with customer's satisfaction	A					2		M
R6	Tech Team Employees	Real	People	3	TalkTalk's Tech team is responsible for managing the network and providing IT support to customers. They also manage security, design products and provide an infrastructure for services.	A	Deliberate act of writing a malicious backdoor code into a program or website, that an engineer may have access too. The backdoor may then be exploited to gain access to sensitive information.	Code being published may not be peer-reviewed properly	L	L	3		H
R7	TalkTalk's Website	Information, Real	Software, Hardware, Data	4	TalkTalk's website provides an interface for its customers to view the available products and provide a range of services. The website's performance and availability can affect TalkTalk's image through the customer's .	A	Deliberate attacks on the website through CSRF, XSS or SQL Injection means to get access to sensitive information	An application or plugin associated with the website or database not up to date and may contain a bug or a vulnerability that can be exploited	H	H	8		H
R8	SQL Database	Information	Data	4	Contains sensitive information belonging to customer.	C,I, A			H	H	8		H
R9	Card Details belonging to Employees/Customers/Company	Information	Data	4	TalkTalk must be in compliance with the Payment Card Industry Data Security Standard, ensuring that stored card details are kept secure and protected. Card details is a popular target for theft, if stolen the impact would affect the company's reputation.	C	There are individuals/organisations that would want to steal card details		H	H	8		H
R10	Personal Information belonging to Employees/Customers/Company	Information	Data	4	Personal Information should be kept secure and protected. Failure to handle this will likely impede GDPR.		There are individuals/organisations that would want to steal sensitive information		H	H	8		H

R11	Software Updates	Information	Software, Procedure	4	Updates can provide immunity to potential vulnerabilities and bugs. Bugs and vulnerabilities are taken advantage of by attackers to get access to any sensitive data.	I	The attacker steals sensitive information through a bug or vulnerability found in the application	Organisation's attitude towards checking the necessary software updates is poor. Some software updates have been avoided since new versions are incompatible with previously written programs	H	H	8	The consequence of this significantly damages TalkTalk's reputation, customers will need to be reimbursed and response efforts will required to ensure existing customers don't leave. [6] This could put stress on employees from customer services and business division. The loss of sensitive data will cause financial losses to both clients and the company. The company must pay a hefty penalty following the breach due to impeding the GDPR.[4] New customers are more unlikely to join TalkTalk, reducing the company's revenue. It will take a long period of time for the company to recover before customers begin to trust the company again. [5] Finances will be used to open an investigation into the incident. If the website was breached then it will have to be shut down affecting availability and putting stress on the tech team. In an event of an espionage further finances will be used to enforce security measures.	H
R12	Staff PCs including netbooks and laptops	Information,Real	Data, Hardware,	3	Computers, laptops and netbooks used by employees may contain sensitive data about themselves or the company.	C,A	In an act of espionage, the attacker could intentionally use a co-worker's PC to get unrestricted access to sensitive information and content	Employees can inadvertently or intentionally let another employee use their personal computer or device giving them potentially unrestricted access to content	H	M	6		H
R13	TalkTalk's Reputation	Intangible	N/A	4	If the customer satisfaction is negatively affected, new or existing customers may leave to join rival companies	I	A security/data breach through any means necessary	Organisation's attitude towards monitoring assets and identifying risks are poor	H	H	8		H
R14	Domain Names	Intangible	Network	4	TalkTalk domain names makes it easy for customers to search for the company through a search engine and tend to be quite memorable. It is of marketing value and is used to establish the company.	A	An attacker can hijack the domain name redirecting users to a malicious site [3]	domain registrar account details not kept secure	H	M	7	Customer services is available to provide services to affected customers. Network engineers can be sent to diagnose any issues and help customers. Response efforts will be required to identify the source of the hijack. [4] [6]	H
R15	TalkTalk Mail	Information	Data, Network	3	TalkTalk mail provides a safe email system for users. Must be maintained and kept secure as email systems are prone to spam and phishing emails.	A	An attacker could potentially steal sensitive information belonging to a user by sending a tailored phishing email to a targeted user.	The platform is susceptible to phishing emails	H	H	7	The consequence of this significantly damages TalkTalk's reputation. [5] The company must contact the registrar to open a domain name dispute,[8] it could take some time before the domain comes back to the company's control. Response efforts will required to ensure existing customers don't leave. This could put stress on employees from customer services and the business division. A long period of time will required for the company to recover from such an attack before customers begin to trust the company again. Expect a huge sum of financial losses.	H
R16	Regular Data Backup	Information	Procedure	2	Helpful to have a backup when there is an unexpected loss of information	I,A	The server that stores the backup may unexpectedly fail and the data becomes permanently lost	Storage device can be damaged by natural disasters	L	L	2	TalkTalk have many secure off-site backup servers to recover data and restore functionality. The impact is the cost in fixing any damages. Customer Services will be available to help any affected customers.	L
R17	Data Centers	Information, Real	Data, Hardware	4	TalkTalk Data Centers are used by many organisations. It is a priority to make sure that the data held is kept safe and the network performance is acceptable otherwise the company's reputation will be negatively affected.	C,I, A			L	L	4		L
R18	Chief Executive Officer	Real	People	4	CEO has access to/knowledge of company's information, meaning that there is a potential for data to be leaked.	A	The CEO could leak company information intentionally or as a result of being blackmailed	The CEO can be a victim of being blackmailed	M	M	6	Leaked information can damage TalkTalk's reputation and the consequence can lead to financial losses for the company.[5] Response efforts need to be established which could lead to further financial losses. [6]There could also be regulation penalties. Recovery time required to gain the trust back of customers.	H
R19	Data Protection Officer	Real	People	3	The Data Protection Officer reviews the company's compliance with GDPR and provides measures and improvements for the organisation to implement	A	Data Protection Officer could intentionally leak areas of weaknesses for attackers to cherry pick and attack	The Data Protection Officer can be a victim of being blackmailed	L	L	3		M
R20	Customer's Router	Real	Hardware	0	If the router fails to work as expected or if it is not secure then it can affect the customer's satisfaction thus affecting TalkTalk's image. The router is easily replaceable and can be installed by an engineer if necessary.	I,A	Attackers could change entries found in the DNS cache in the router. The user will be redirected to a malicious website by the DNS server. [7]	The DNS tables in the router can be manipulated to reroute domain names to a different ip address	L	M	1	Not much of an impact, customer services is available to provide services to affected customers. Network engineers can be sent to diagnose any issues and help customers. If the number of cases of cache poisoning becomes large then expect damages to the company's reputation. Response efforts will be required to replace routers for free and provide any help.	L
R21	Blueprints	Intangible	Data	2	They can provide an advantage to organisations or an individual if in the wrong hands. The company's security will be breached if blueprints were leaked.	C	There are individuals/organisations that would want to steal blueprints	Valuable asset to an organisation or individual willing to steal the blueprints	L	L	2	Enforce tight security. Financial losses for the company due to the installation of tight security and some response efforts, such as an investigation into the matter. Media attention could affect company's reputation.	L

1.A | My Prioritised Risks

Risk	Asset	Asset Value (0-4)	Threat	Vulnerability	Ease of Exploitation	Likelihood of threat occurrence	Risk Scores from Table E.1	Business Impact	Impact LHM
R9	Card Details belonging to Employees/Customers/ Company	4	There are individuals/organisations that would want to steal card details	An application or plugin associated with the website or database not up to date and may contain a bug or a vulnerability that can be exploited	H	H	8	The consequence of this significantly damages TalkTalk's reputation, customers will need to be reimbursed and response efforts will required to ensure existing customers don't leave.[6] This could put stress on employees from customer services and business division. The loss of sensitive data will cause financial losses to both clients and the company. The company must pay a hefty penalty following the breach due to impeding the GDPR. [4] New customers are more unlikely to join TalkTalk, reducing the company's revenue. It will take a long period of time for the company to recover before customers begin to trust the company again. [5] Finances will be used to open an investigation into the incident. If the website was breached then it will have to be shut down affecting availability and putting stress on the tech team. In an event of an espionage further finances will be used to enforce security measures.	H
R10	Personal Information belonging to Employees/Customers/ Company	4	There are individuals/organisations that would want to steal sensitive information		H	H	8		H
R7	TalkTalk's Website	4	Deliberate attacks on the website through CSRF, XSS or SQL Injection means to get access to sensitive information		H	H	8		H
R8	SQL Database	4			H	H	8		H
R11	Software Updates	4	The attacker steals sensitive information by utilizing a bug or vulnerability found in the software that had not been updated	Organisation's attitude towards checking the necessary software updates is poor. Some software updates have been avoided since new versions are incompatible with previously written programs	H	H	8		H

1.B | Risk Treatment Plan

Risk	Asset	Asset Value (0-4)	Threat	Vulnerability	Risk Scores from Table E.1	Control Strategy	Control	Control	Ease of Exploit	Likelihood of threat Occurrence	Risk Score from Table E.1	Business impact	Impact LHM
R9	Card Details belonging to Employees/Customers/ Company	4	There are individuals/organisations that would want to steal card details	An application or plugin associated with the website or database not up to date and may contain a bug or a vulnerability that can be exploited	8	Transfer	C1	Details can be outsourced to 3rd party organisations such as Amazon AWS or Firebase	L, must pay 3rd party for their services	M	5	The fault of the problem will be Amazon AWS/Firebase's. There will still be residual reputational impact on TalkTalk	L
						Overlaps with R7, R8 & R11	C2	Duplicate of C5 and C8					
R10	Personal Information belonging to Employees/Customers/ Company	4	There are individuals/organisations that would want to steal sensitive information		8	Overlaps with R9. R8	C3	Duplicate of C1					
						Overlaps with R7, R8 & R11	C4	Duplicate of C5 and C8					
R7	TalkTalk's Website	4	Deliberate attacks on the website through CSRF, XSS or SQL Injection means to get access to sensitive information		8	Defence	C5	A web application firewall can be implemented to filter malicious data providing a defence against sql attacks. Introduce an anti-forgery token so that the server can only accept a http request with a valid token preventing csrf attacks. Lastly go through the web application code and escape all user's input, html, url and javascript. Ensure that all user input is validated to prevent XSS/javascript/sql injection. [9]	L, prevents malicious attacks on the website	M	5	Remains Unchanged	H
						Overlaps with R11	C6	Duplicate of C8					
R8	SQL Database	4			8	Overlaps with R9, R10	C7	Duplicate of C1					
R11	Software Updates	4	The attacker steals sensitive information by utilizing a bug or vulnerability found in the software that had not been updated	Organisation's attitude towards checking the necessary software updates is poor. Some software updates have been avoided since new versions are incompatible with previously written programs	8	Defence	C8	Put together a system management team that will regularly check if software is up to date. Additionally the team will also be responsible for identifying any vulnerabilities and bugs in the the system's code. Proactively monitor the database for any security/performance related issues to identify breaches quicker	L, vulnerabilities are fixed by updating software and maintaining code	L	4	Remained Unchanged	H

1.C | Control Recommendations and Assessment

Control	Control	Previous Risk Priority	New Risk Priority	Assessment	Recommendation
C1	Details can be outsourced to 3rd party organisations such as Amazon AWS or Amazon AWS or Firebase	8	5	This removes the company's responsibility of keeping the data secure as its responsibility is now passed to Amazon AWS (example of a 3rd party organisation). The risk of the data being breached is reduced since Amazon is a well known company, however the drawbacks is that there is an up-keep, and payments need to be made on a monthly bases. Many different services and products rely on the current database that TalkTalk have and therefore will need to be reworked to accommodate the new cloud database. This control is to be AVOIDED since the costs of switching database would be significant. Lastly they will still be some degree of reputational impact on TalkTalk if attackers manage to steal data from the cloud services.	The business team can investigate the benefits and drawbacks of switching the database. Although as it stands the company should focus on implementing control 5 and 8 as they reduce risks R7, R8, R9. R10. R11, R2, R13 and provides a better alternative to this control.
C5	A web application firewall can be implemented to filter malicious data providing a defence against sql attacks. Introduce an anti-forgery token so that the server can only accept a http request with a valid token preventing csrf attacks. Lastly go through the web application code and escape all user's input, html, url and javascript. Ensure that all user input is validated to prevent XSS/javascript/sql injection.	8	5	This control removes the vulnerabilities and bugs that exists within the company's website. The risk has been reduced significantly by introducing measures to prevent common attacks. Introducing this control will improve the defences, and will reduce the threat of attackers stealing customer's card details and sensitive information (helps reduce risks R9, R10 & R13). The only expense is that the website will need to be taken down to implement any changes and the cost of staff time. It's important that C8 is implemented so that software is kept up to date and the site is actively monitored for any faults.	This project should be completed as soon as possible to reduce the threat occurrence, it will need to be carefully executed and managed by a technical team who has knowledge on OWASP top ten. Maintenance can be done every X number of days at midnight to push any changes. Customers should be notified of such maintenance work.
C8	Put together a system management team that will regularly check if software is up to date. Additionally the team will also be responsible for identifying any vulnerabilities and bugs in the the system's code. Proactively monitor the database for any security/performance related issues to identify breaches quicker	8	4	This control removes any vulnerabilities/bugs within the website by updating the software and making any appropriate changes. Updating the software reduces the number of attacks, reducing the chances of getting attacked. By proactively monitoring the database the system management team can identify any security breaches and respond much faster, alleviating any damages before it get much worse. This control reduces the following risks; R8, R7, R9, R10, R13 & R2.	Updating software could lead to more risks and errors since updating the current legacy SQL database may result in incompatibilities. Commence a long term project to update the project to the latest version, this will be assigned to a technical team of engineers. This control can be in conjunction with C5, but it's recommended to solve the underlying issue of updating the database initially. The team should regularly consult to determine the scope, requirements and errors that persists.

2. ISO/IEC27005 vs NIST RIsk Assessment

ISO 27005 standard is a suitable guidance for TalkTalk to manage the risks that could very well compromise it’s information security. The standard can adopt a component-driven or system-driven approach in risk management, but falls closer to a component-driven methodology due to its element of risks being comprised of impacts, vulnerabilities and threats. Both frameworks are component oriented but there are some key features that make the ISO 27005 framework better. [11] The NIST risk assessment handles risk management which can be summarised in 4 steps: preparing the assessment, conducting assessment, communicating the results and the maintenance of the assessment. [13] Each step is thoroughly detailed and clear making it easy for an organisation to follow. This could pose a problem for an organisation that require more flexibility in order to meet their own requirements. On the other hand ISO 27005 framework handles the management similarly dividing the process into 3 main steps: risk identification, risk analysis and risk evaluation, each defined briefly in a concise, clear manner offering flexible whereas NIST does not. [10] [12] ISO 27005 framework is a generic risk management approach that can be shaped into the perfect guide capable of delivering TalkTalk’s requirements. [10] TalkTalk also has a large number of personnel including a Data Protection Officer that can be utilized to tailor the implementation for the company. Another key difference between the two frameworks is that the ISO 27005 framework can be used more generally in the sense that human resources are considered assets, whereas NIST is much technical and would not consider human resources as an asset. [10] It could be beneficial to implement more than one framework if resources are available to do so. The company could use another framework such as the OCTAVE framework to qualitatively analyse the assets. Octave uses qualitative measurements to identify critical assets and their security requirements. Threats and impacts are identified and strategies are drawn to mitigate the risks. [10] I believe that ISO 27005 framework is best suited for the organisation needs and should not consider the NIST risk management framework since it is aimed for organisations that are largely based in the U.S. The steps are very detailed compared to the ISO 27005 framework but does not consider any regulations and laws that are based in the UK, where TalkTalk is based.It's important to understand that there exists no framework where every risk can be identified. [10] The framework should be selected based on the company’s requirements such that through an iterative process, risks can narrowed down to help make key decisions in managing and controlling risks effectively.

References

[1] Derek Manky (8/11/2010) “Top 10 vulnerabilities inside the network” [Online], Available at https://www.networkworld.com/article/2193965/top-10-vulnerabilities-inside-the-network.html [Accessed: 22/11/2019]

[2] finjanmobile.com (25/01/2018) “The Dangers of Using Unsecured Wi-Fi” [Online], Available at https://www.finjanmobile.com/the-dangers-of-using-unsecured-wi-fi/ [Accessed: 23/11/2019]

[3] imperva.com “Domain name server (DNS) Hijacking” [Online], Available at https://www.imperva.com/learn/application-security/dns-hijacking-redirection/ [Accessed: 23/11/2019]

[4] FirstData “Small Businesses: The Cost of a Data Breach Is Higher Than You Think” [Online], Available at https://www.firstdata.com/downloads/thought-leadership/Small_Businesses_Cost_of_a_Data_Breach_Article.pdf [Accessed: 23/11/2019]

[5] Mark Di Somma “10 Brand Threats And How To Counter Them” [Online], Available at https://www.brandingstrategyinsider.com/2016/02/10-brand-threats-and-how-to-counter-them.html#.XeR8ujL7TpA [Accessed: 24/11/2019]

[6] Annabelle Graham “The damaging after-effects of a data breach” [Online], Available at https://www.itgovernance.co.uk/blog/the-damaging-after-effects-of-a-data-breach [Accessed: 24/11/2019]

[7] StackOverflow “How easy/difficult is it to spoof DNS? Are some scenarios safer/more risky than others?” [Online], Available at https://security.stackexchange.com/questions/6827/how-easy-difficult-is-it-to-spoof-dns-are-some-scenarios-safer-more-risky-than#:~:targetText=If%20the%20victim%20is%20using,it%20is%20trivial%20to%20spoof. [Accessed: 26/11/2019]

[8] SecurityTrails “Preventing Domain Hijacking – 10 Steps to Increase your Domain Security” [Online], Available at https://securitytrails.com/blog/preventing-domain-hijacking-10-steps-to-increase-your-domain-security [Accessed: 27/11/2019]

[9] Sarah Vonnegut “3 Ways to Prevent XSS” [Online], Available at https://www.checkmarx.com/2017/10/09/3-ways-prevent-xss/ [Accessed: 27/11/2019]

[10] itgovernance.co.uk (16/05/2019) “Why ISO 27005 risk management is the key to achieving ISO 27001 certification” [Online], Available at https://www.itgovernance.co.uk/blog/why-iso-27005-risk-management-is-key-to-iso-27001 [Accessed: 30/11/2019]

[11] nvsc.gov.uk (8/08/2016) “Risk management guidance” [Online], Available at https://www.ncsc.gov.uk/collection/risk-management-collection [Accessed: 30/11/2019]

[12] International Standard (2018) "Information technology - Security techniques - Information security risk management", [Online], Available at https://www.sis.se/api/document/preview/80005503/ [Accessed: 31/11/2019]

[13] NIST U.S. Department of Commerce (Sept 2012) “Information Security” [Online], Available at https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf [Accessed: 31/11/2019]