Toby bluck

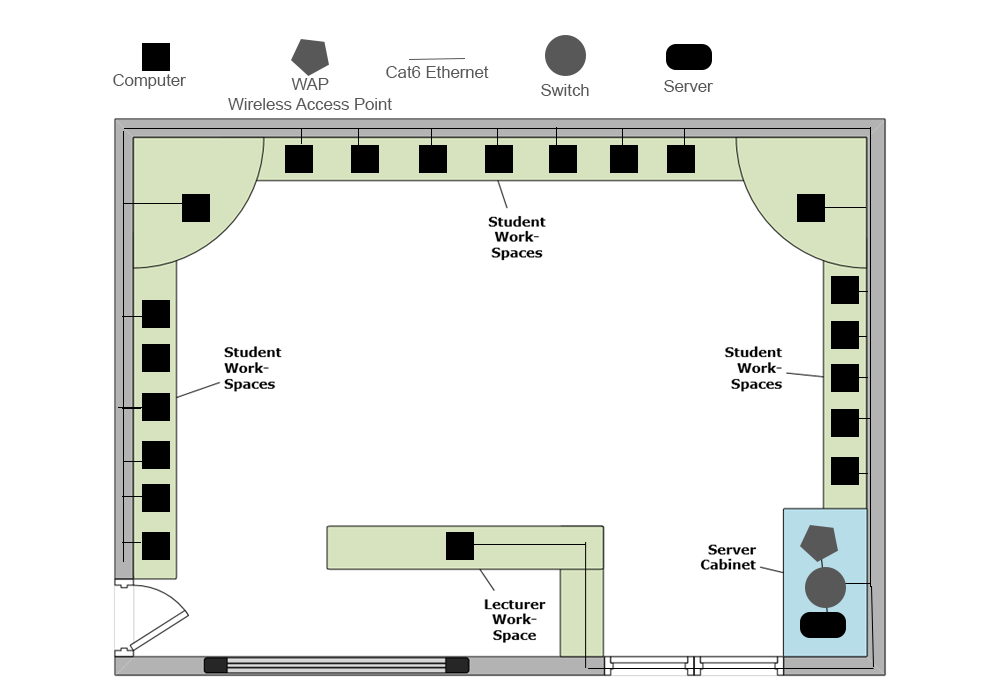
bLU16274423  2053 Words

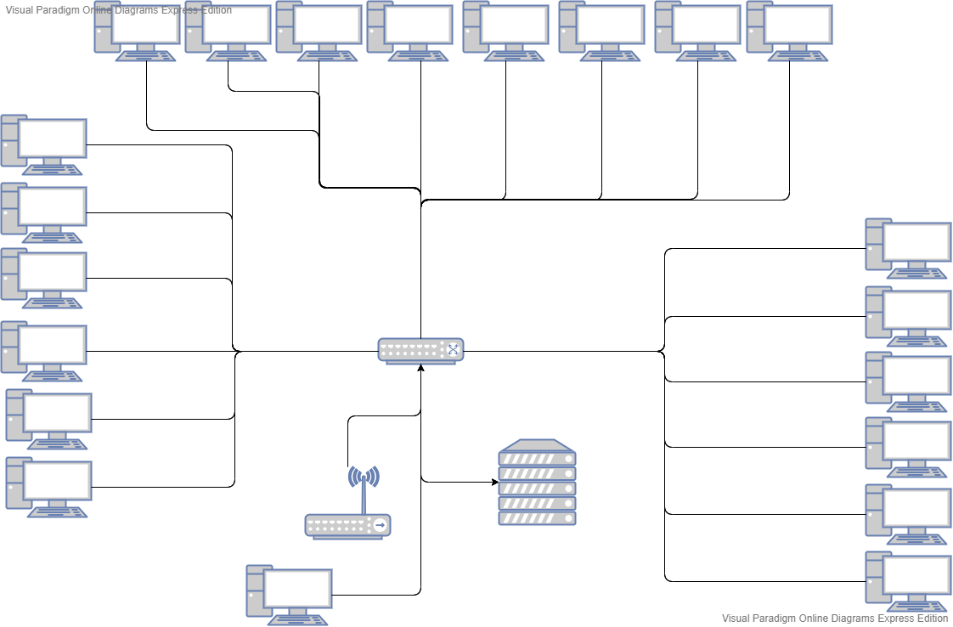
SCDT43 CW2  
Network Planning, Design and Implementation, Including a Cyber Risk Assessment

# Topology design:

Due to the lab being a singular entity to the college local area network, it requires no communication or connectivity to it. Furthermore, due to this is does not need to be as robust as the college’s local network but still needs to be scalable and functional is one or more system/s is unusable. The most optimal topology to be implemented within the lab would be a star topology. (Faircloth, 2014)

# Layout plan & topological design:





# Cost of hardware:

Server & Switch – 1 x Dell EMC PowerEdge T440 = £1233.31 & 1 x Cisco Catalyst 2960S-F24TS-L = £1,161.59 (Direct, 2020) (Insight, 2020)

Cabling – 1 x Cat6 UTP PVC Solid Cable 305 Metres = £113.22 & 69 x Cat6 3 50-micron RJ45 Crimp Plug = £24.84 (Monkey, 2020) (Ltd, 2020)

WAP – 1x NETGEAR WAC104 = £63.59 (Insight, 2020)

Total cost for the hardware = £2596.55

# Justification:

Layout –

All systems are placed at a location where it will provide the students which enough space, and keeping the systems out of students way to keep the floor free from obstructions as per HSE guidelines (Health & Safety Executive UK) (Have the right workplace facilities: What you must provide for a safe and healthy workplace - HSE, 2020)

all networking related cabling will to be to a socket from the system, which is run through trunking alongside the wall and leads to the switch, this allows for the cables coming from the system to be replaced easily as they would most likely to be damaged.

Furthermore, PAT testing should be done with all systems as part of a safe deployment, as per regulations. (PAT Testing Regulations - PAT Testing, 2020)

Following Cisco’s guidelines for cable management, related cables should be bundled together. This allows for a better organisation of cabling from the switch to dedicated areas. (Systems, 2013)

Overall, this solves many problems and provides many benefits regarding the layout in the lab.

Layout of the networking cables within the lab will allow for a better maintenance within the future of the network, alongside better cabling can improve the airflow within the server cabinet. The layout diagram present also allows for enough space for people to access the door in case of an emergency keeping up to HSE standards. (HSE, 2020) (White, 2016)

Topology –

As the lab LAN needs to be high speed and isolated this topology is suitable due to the simplicity of the star topology, alongside the additional benefits of the topology being highly scalable. There are potential flaws to this however, the positives of this topology outweigh the negatives. With the lab being isolated, the addition of extra computers would be relatively easily to add to the network, as the switch would act as the core of the network meaning only one direct connection would be required or on the opposite a system can easily be removed without causing issues in the network.

Furthermore, the overall diagnostics of issues within the network using this topology is extremely simple, per say is a system was not available on the network, you could inspect the networking cables for damage etc or going straight to the switch for the diagnosis. Modification of the lab network with the star topology would be easily if it needed to be extended further it could be an extended star. (Faircloth, 2014), (Pandya, 2013)

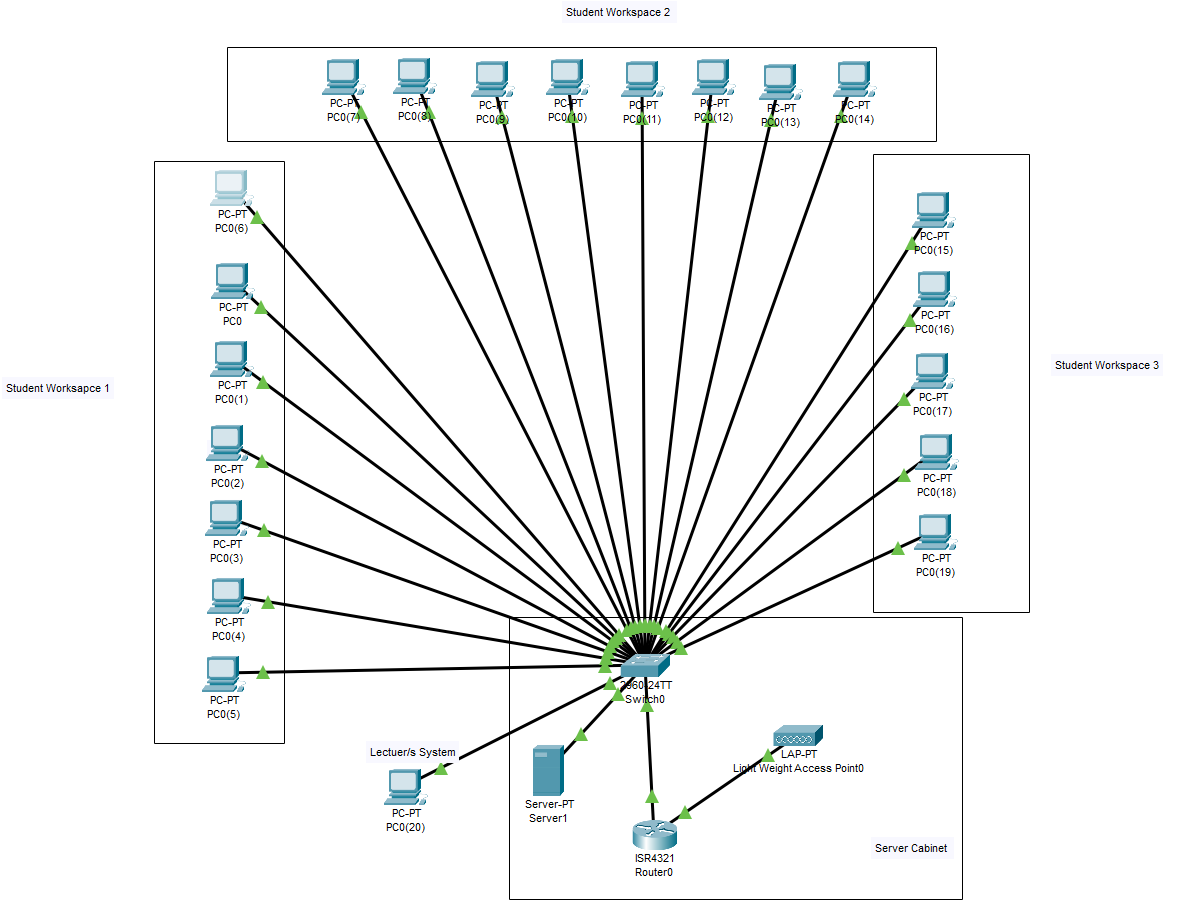
Architecture

For the physical side of the network within the lab the architecture that would be most beneficial and suitable for this would be client server side, this will fit the requirements as the server will act as the centralized hub which controls the traffic and will have control over the network meaning that it will be able to manage the active directory and group policies needed for the network. As the server in the lab will act as a file server its beneficial to use this as the systems will be able to request data from the server and compile the data sent opposed to the server doing it will is greatly helps the reduce the overall network traffic while retaining the best performance it can. (Liu, 2009) (Gough, 2011)

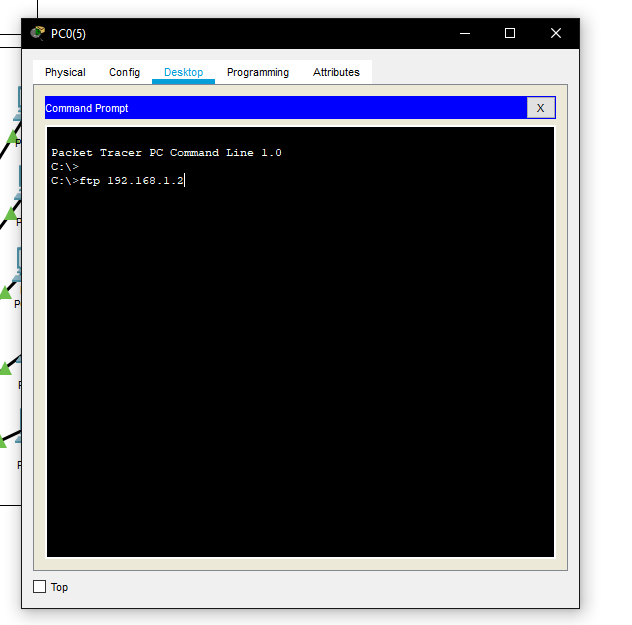
## Wireless network architecture

Within the lab, a WAP will be present allowing for a wireless network to be formed, using the star topology a star architecture will also be utilised for the wireless network, this is due to the overall reliability, as the WAP is based in the lab all devices within the lab will be able to achieve a strong wireless connection further adding to its reliability. Furthermore, as there is only one hop needed for this from a central hub to the node it is very efficient.(Walrand & Varaiya, 2000)

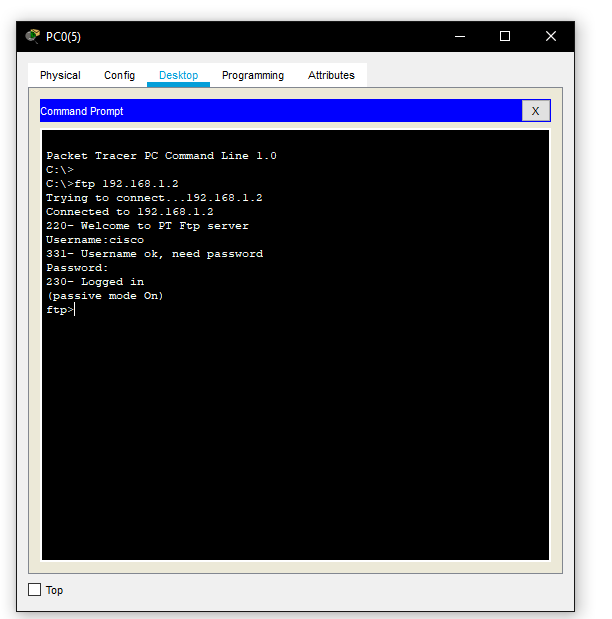
# Packet tracer & testing:



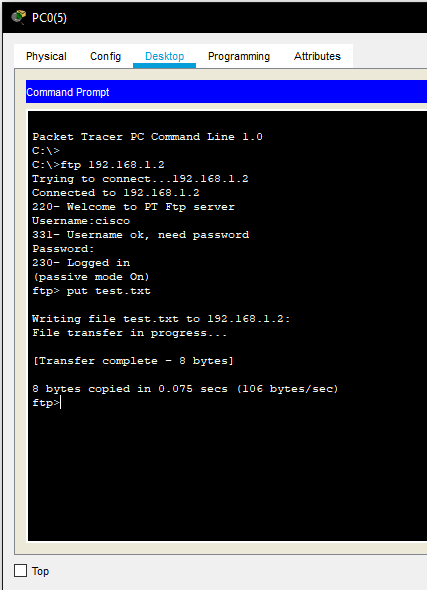
Packet tracer diagram of the lab network that has broken down into what is stored into the server cabinet (server, router, WAP and switch) and the student work desks which has the PCs. All the computers are using a Gigabit ethernet connection to the switch allowing for high speed connectivity.



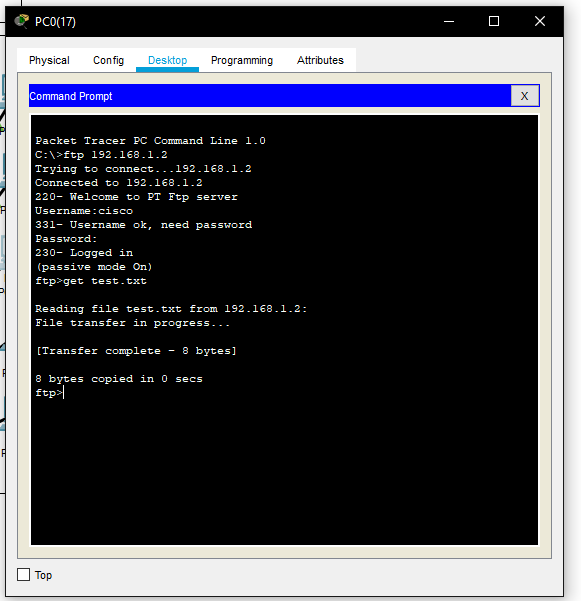
Testing the FTP connection to the server by using the command console.



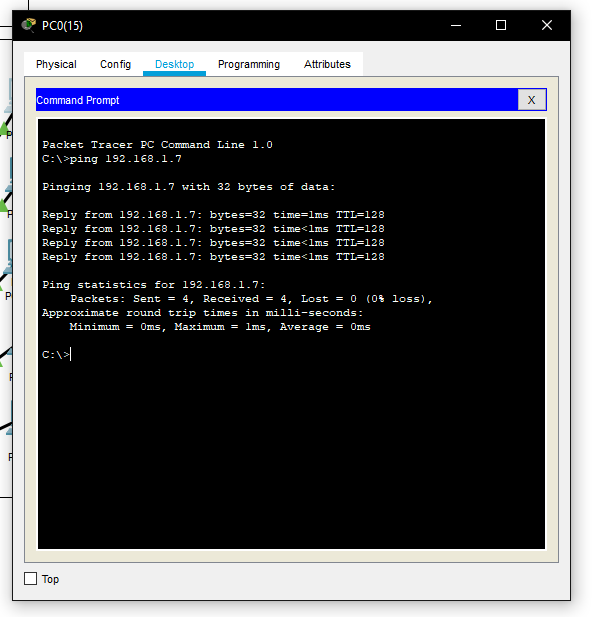
Once the connection has established with the server you can log into the ftp with a username and password this is where you can upload files to the server for the other PCs to access.



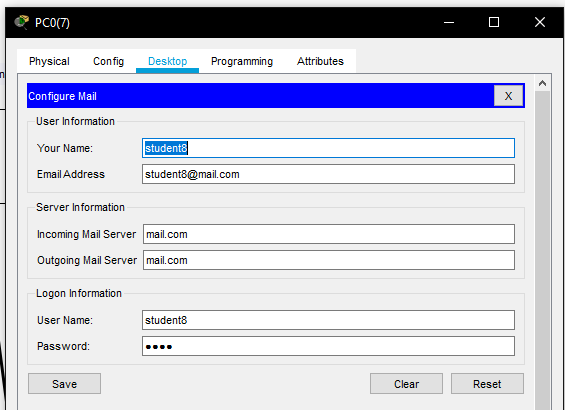
Sending a file from the computer to the server using ftp with the amount transferred and the time it took for the transfer to be completed.



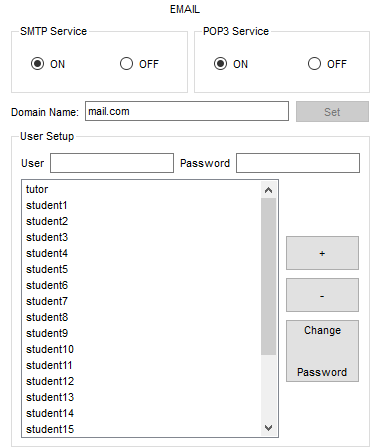
This is using the FTP to access the server and pulling files stored on the server to the PC using the FTP command.



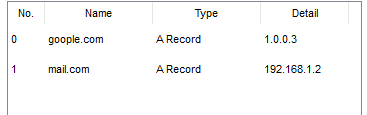
This is a test where you can see that the computers can communicate between one another.



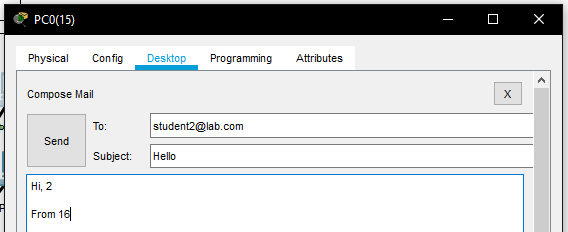
Configuration of the email on an individual system showing the incoming and outgoing server as well as the email address and a login for the student PC.



The configuration of the email domain and the adding of clients with their username and password which was set up on each of the student’s PC within the lab.



DNS set up for the mail.com domain for the students to freely send and receive emails to one another.



Sending of email to a student from a different PC where they will be able to communicate to each other.

# Cyber security risk assessment:

## Analysis of information value-

### Areas-

* Physical Assets: Computers, Network equipment and Wires.
* Virtual Assets: Plans, Databases and Files.
* Documents: Documentation and Procedures.
* Services: Computer or network services.
* Software: Applications, Development tools and Support software.

Financial or legal penalties that can be enforced on UCS such as GDPR which has a 4% of the annual revenue or up to 20 million Euro. Other authorities such as the ICO (Information Commissioner’s Office) can distribute other punishments too such as: monetary penalty fines £1000, Enforcement Notices to comply with.

Information of worth for competitor/s is generally not applicable in these circumstances unless exceptional one of cases. +

Loosing this information impacts UCS both on minor and major scales, dependant on information lost, such as personal data i.e. personal logins, student info which would fall under GDPR legislation other data like configuration other files would fall under minor.

Impact of day to day operations dependant on the scale of damage/issues the operations of the lab may not be affected or limited services on the systems to being un-operational.

Reputational damage any form of threat or accident in the lab could reflect on UCS and cause reputational damage in which could be off-putting to potential employee or students in the future etc.

### Using the above areas, a questionnaire to calculate value of information within the lab/UCS:

|  |  |  |
| --- | --- | --- |
| Section & Question | Answer | Score |
| Loss of Information - what happens without the information | Nothing  Minor to little inconvenience  Replaceable but noticeable loss/inconvenience/issues  Costs are incurred to replace or fix information loss related issues  Need to procure information, stopping of lab network too campus network – Law/s or legislations involved | 0  1  2  3  4 |
| Value -  cost of the gathering or acquire new information | None to very small  Some degree of costs but not high or low  High cost  Very high cost  Incredible high cost | 0  1  2  3  4 |
| Time –  Does information depreciate in value in regard to the interest of UCS | Depreciates extremely quickly  Fairly quick  Up to a year  Depreciates after a year too years  Never depreciates | 0  1  2  3  4 |
| Legislations/Law -  Regulations for the information being kept by UCS/Lab and implications caused if lost/destroyed | None  Necessary to keep data for a short timeframe  Needs to hold information, but without implications  Mandatory data storage and can carry small penalties  Mandatory data storage and can breach laws | 0  1  2  3  4 |

(Sajko et al., 2006) (Tunggal, 2020) (Kassa, 2017) (Ayo et al., 2020)

## Asset prioritisation-

|  |  |
| --- | --- |
| Total value of information (score) | Importance |
| 0 – 5 | Low importance, that will carry little to consequences in UCS |
| 6 – 10 | High importance, sufficient measures in place to avoid issues and facing consequences. |
| 11 – 16 | High value information/assets in UCS, all necessary measure in place to protect and/or store, heavy consequences are will be enforced. |

(Sajko et al., 2006) (Tunggal, 2020) (Kassa, 2017) (Ayo et al., 2020)

## Identification of potential threats and identified vulnerabilities:

### Threats –

* Viruses, trojans, worms, malware etc.
* Physical attacks
* Zero-day exploits
* Insiders
* Natural disasters
* Hacking

(kaspersky, 2020) (Cisco, 2020) (Abomhara & Koien, 2015) (ICAEW, 2020)

### Vulnerabilities –

* Command injection
* Access groups, privileges etc.
* Weak network design
* Network security
* Power disturbance
* Authentication
* Logging and monitoring being sub-par

(Khan & Gouvia, 2017) (Security, 2011) (OWASP, 2017)

## Prioritisation of the likelihood and impact of identified risks-

### Likelihood of risks:

|  |  |
| --- | --- |
| Likelihood | Meaning |
| 1 | Possibility is almost non-existent to happen |
| 2 | Possibility is remarkable unlikely to happen |
| 3 | Possibility is highly unlikely to happen |
| 4 | Somewhat unlikely to happen |
| 5 | Possible but low chance of happening |
| 6 | Possibility to happen |
| 7 | Pretty possible to happen |
| 8 | Chances to be expected of it happening |
| 9 | High chance of it happening |
| 10 | Extremely likely to happen |

### Impact of identified risks:

|  |  |  |
| --- | --- | --- |
| Risks | Description | Likelihood |
| Viruses, trojans, worms, malware etc. | Destruction of systems, network and data. | 5 |
| Physical attacks | Breaking of locks, physical damage of components etc. | 3 |
| Zero-day exploits | Issues with equipment and potential for loopholes or security breaches | 4 |
| Insiders | Damage or risk of data being compromised | 4 |
| Natural disasters | Destruction of equipment and data within lab | 5 |
| Hacking | Stealing of data or hijacking of network | 4 |
| Command injection | Malicious damage to the network and data within the lab | 2 |
| Access groups, privileges etc. | Users may have access to folders they aren’t allowed to access. | 6 |
| Weak network design | This allows for attacks within the network infrastructure easily allowing for data or other information to be stolen | 2 |
| Network security | Remote connection bypass firewall allowing for data to be damaged/stolen causing damages/downtime. | 5 |
| Power disturbance | Loss of data and potential configuration set up | 3 |
| Logging and monitoring being sub-par | Early detection of intruders will not be captured allowing for anything to happen within the network | 6 |

[(Ayo et al., 2020)](https://arxiv.org/ftp/arxiv/papers/1812/1812.04659.pdf 722)

Resolution/control advice for identified risks- 323- 550 words.

Physical controls –

Physical security on areas that hold items or store data, this can be limited to locks on the server cabinet and locks on the panels of the student computers. Card readers for the locking mechanism on the doors so only students and/or tutors can unlock the door to the lab this will reduce the chance of physical attacks. Furthermore, to reduce any data or power disturbances a UPS (Uninterrupted Power Supply) will allow for a period to be ran which out any other power going directly to the systems.

### Technical and admin controls -

The network should have well configured firewalls to prevent attacks and increase network security, one before the latest update in the server OS to prevent any zero-day exploits, anti-virus/ malware/ spyware software to prevent any information being stolen. Enough logging of the server to review for any anomalies as well as local and offsite back-ups to prevent data loss in numerous situations such as natural disasters etc.

Sufficient access groups with relative privileges to be applied to all accounts to prevent any insider abuse on the labs systems and network. Software should be in place to record and log who uses what system and whether any outsiders from the lab have had access. Policies for the lab can be implemented to prevent any issues with handling important data, general use, disaster plans, breaching this allows for both measure to be in place and ready as well as conforming both to internal policies in UCS and legal policies. supervision of students should be undertaken by a tutor to make sure that no foul play can happen which would reduce any insider attack such as command injection etc. appropriate training for the tutors of the lab to keep them updated on knowledge and security measures and information. A strong wireless password should be used to prevent hacking over WIFI using WPA2.

Controls should be reviewed on a regular basis to update the controls for the risks and minimise them and implement new methods to subdue them. Minimising smaller lesser risks is important but cannot be completely accounted for as this can be due to human error and can only be limited to a certain amount, however those risks will pose little threat to the UCS and Lab environment and cause more of an inconvenience. (Miller, 2016) (Ayo et al., 2020)

2053 words

# References:

Abomhara, M. and Koien, G. (2015) Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks, Journal Of Cyber Security And Mobility, vol. 4, no. 1, pp. 65-88.

Ayo, S., NGALA, B., AMZAT, O., KHOSHI, R. and MADUSANKA, S. (2020) 1Information Security Risks Assessment: A Case Study, [Online]. Available at <https://arxiv.org/ftp/arxiv/papers/1812/1812.04659.pdf>.

Cisco (2020) Cyber Attack - What Are Common Cyberthreats?, Cisco, [Online]. Available at <https://www.cisco.com/c/en_uk/products/security/common-cyberattacks.html#~definition>.

Direct, S. (2020) Dell EMC PowerEdge T440 Xeon Silver 4110 2.1 GHz 16GB - 600GB Tower Server on Servers Direct, Serversdirect.Co.Uk, [Online]. Available at <https://www.serversdirect.co.uk/p/1283771/dell-emc-poweredge-t440-xeon-silver-4110-2.1-ghz-16gb-600gb-tower-server>.

Faircloth, J. (2014) Enterprise Applications Administration,.

Gough, M. (2011) How To Cheat At Voip Security, Syngress.

Have the right workplace facilities: What you must provide for a safe and healthy workplace - HSE (2020) Hse.Gov.Uk, [Online]. Available at <https://www.hse.gov.uk/simple-health-safety/workplace-facilities/welfare.htm>.

HSE (2020) Workplace Health, Safety And Welfare: A Short Guide For Managers, Health and Safety Executive [Online]. Available at <https://www.hse.gov.uk/pubns/indg244.pdf>.

ICAEW (2020) Top Five Cyber Risks, ICAEW [Online]. Available at <https://www.icaew.com/-/media/corporate/files/technical/business-and-financial-management/smes/bas-files/top-five-cyber-risks.ashx?la=en>.

Insight (2020) Cisco Catalyst 2960S-F24TS-L... | WS-C2960S-F24TS-L | £967.99 | Insight UK, Uk.Insight.Com, [Online]. Available at <https://www.uk.insight.com/en-gb/productinfo/network-switches/0001746945-00000001>.

Insight (2020) NETGEAR WAC104 - radio access po... | WAC104-100UKS | £52.99 | Insight UK, Uk.Insight.Com, [Online]. Available at <https://www.uk.insight.com/en-gb/productinfo/id/0006529369>.

kaspersky (2020) What is Cyber Security?, Kaspersky.Co.Uk, [Online]. Available at <https://www.kaspersky.co.uk/resource-center/definitions/what-is-cyber-security>.

Kassa, S. (2017) IT Asset Valuation, Risk Assessment and Control Implementation Model, ISACA Journal, vol. 3, [Online]. Available at <https://www.isaca.org/resources/isaca-journal/issues/2017/volume-3/it-asset-valuation-risk-assessment-and-control-implementation-model>.

Khan, S. and Gouvia, L. (2017) Cybersecurity Attacks: Common Vulnerabilities in the Critical Infrastructure, IPASJ International Journal Of Computer Science, vol. 5, no. 6, [Online]. Available at <http://researchgate.net/publication/319800931_Cybersecurity_Attacks_Common_Vulnerabilities_in_the_Critical_Infrastructure>.

Liu, D. (2009) Cisco Router And Switch Forensics, Burlington, MA, Syngress.

Ltd, C. (2020) Netshop, Netshop.Co.Uk, [Online]. Available at <https://www.netshop.co.uk/products/cat6-3-50-micron-rj45-crimp-plug-universal-round>.

Miller, S. (2016) A Cyber Security Risk Assessment Of Hospital Infrastructure Includingtls/SSL And Other Threat, Queen's University Belfast [Online]. Available at <https://pureadmin.qub.ac.uk/ws/portalfiles/portal/125120790/StuartMillar13616005_ACyberSecurityRiskAssessmentOfHospitalInfrastructure_TLS.pdf>.

Monkey, C. (2020) Cat6 UTP PVC Solid Cable (Reel) | Cat6 Cable, Cablemonkey.Co.Uk, [Online]. Available at <https://www.cablemonkey.co.uk/cat6-cable/21-excel-cat6-utp-cable.html#/56-length-305mt>.

OWASP (2017) OWASP Top 10 -2017, OWASP [Online]. Available at <https://owasp.org/www-pdf-archive/OWASP_Top_10-2017_%28en%29.pdf.pdf>.

Pandya, K. (2013) Network Structure or Topology, International Journal Of Advanceresearch Incomputer Science And Management Studies, vol. 1, no. 2, [Online]. Available at <http://ijarcsms.com/docs/paper/volume1/issue2/V1I2-0006.pdf>.

PAT Testing Regulations - PAT Testing (2020) PAT Testing, [Online]. Available at <https://www.pat.org.uk/pat-testing-regulations/>.

Sajko, M., Bača, M. and Rabuzin, K. (2006) How to calculate information value for effective security risk assessment, Journal Of Information And Organizational Sciences, [Online]. Available at <https://www.researchgate.net/publication/26596362_How_to_calculate_information_value_for_effective_security_risk_assessment>.

Security, H. (2011) Common Cybersecurity Vulnerabilities In Industrial Control Systems, Homeland Security [Online]. Available at <https://www.us-cert.gov/sites/default/files/recommended_practices/DHS_Common_Cybersecurity_Vulnerabilities_ICS_2010.pdf>.

Systems, C. (2013) Guidelines And Best Practices For The Installation And Maintenance Of Data Networking Equipment, [Online]. Available at <https://www.cisco.com/c/dam/en_us/training-events/downloads/guidelines_and_best_practices_for_the_Installation_and_maintenance_of_data_networking_equipment.pdf>.

Tunggal, A. (2020) How to Perform an IT Cyber Security Risk Assessment: Step-by-Step Guide, Upguard.Com, [Online]. Available at <https://www.upguard.com/blog/cyber-security-risk-assessment>.

Walrand, J. and Varaiya, P. (2000) High-Performance Communication Networks, 2nd ed. San Francisco, California, Morgan Kaufmann Publishers.

White, R. (2016) Benefits to Cable Management – IT Industry, Linkedin.Com, [Online]. Available at <https://www.linkedin.com/pulse/benefits-cable-management-industry-rob-white>.