William Adoukonou

[Company name]  [Company address]

Emerging Trends in cyber security  
  
assignment 1

Contents

[Introduction 2](#_Toc187154191)

[Task 1 – Evaluate how the following emerging trends are beneficial for organisation to develop cyber security infrastructure. 3](#_Toc187154192)

[Cloud Computing 3](#_Toc187154193)

[Blockchain 5](#_Toc187154194)

[Genesis Blocks 5](#_Toc187154195)

[Blockchain Tampering 6](#_Toc187154196)

[Virtualisation 6](#_Toc187154197)

[Benefits and Drawbacks of Virtualization 6](#_Toc187154198)

[Current Trends 7](#_Toc187154199)

[Zero Trust Security Models 7](#_Toc187154200)

[Biometrics and Behavioural ID 7](#_Toc187154201)

[Challenges 7](#_Toc187154202)

[Dealing with systemic and complex risks 8](#_Toc187154203)

[Hybrid Threats 8](#_Toc187154204)

[Impacts 9](#_Toc187154205)

[Economic 9](#_Toc187154206)

[Reputational 9](#_Toc187154207)

[Legal Consequences 9](#_Toc187154208)

[Task 2 - Critically evaluate appropriate tools for developing organisation cyber security systems for businesses of all sizes 11](#_Toc187154209)

[Firewalls 11](#_Toc187154210)

[Penetration Testing 12](#_Toc187154211)

[Create a 4-week cyber security industrial plan 14](#_Toc187154212)

[Step 1 - Create a poster to promote cyber security at UCB 14](#_Toc187154213)

[Step 2 – Create a Phishing Prevention email 15](#_Toc187154214)

[Step 3 – Importance of MFA implementation in the staff members 16](#_Toc187154215)

[Step 4 – An email on how to protect staff from further threats 17](#_Toc187154216)

[Conclusion 18](#_Toc187154217)

# Introduction

Emerging trends are new technologies that are becoming more commonplace in the cyber security industry. This assignment will document some of them: Cloud computing and Blockchain. This will help explain what direction the industry is heading in. This assignment will also go over current trends such as Zero Trust and biometric verification like facial and fingerprint scanners. It will evaluate their benefits and drawbacks when looking for a defence to complex and advanced threats to UCB’s network. To reiterate the issues with poor cyber security, I will explain how UCB would suffer legal, economic, and reputational impacts.

Task 2 will look further into the hardware that UCB can use and what components are the current standard in the industry. This will go alongside a four-week plan that has been created to increase overall awareness of cyber security across the university. Using social media and staff emails, UCB can bring more awareness to cyber security tech such as MFA and Phishing.

# Task 1 – Evaluate how the following emerging trends are beneficial for organisation to develop cyber security infrastructure.

## Cloud Computing

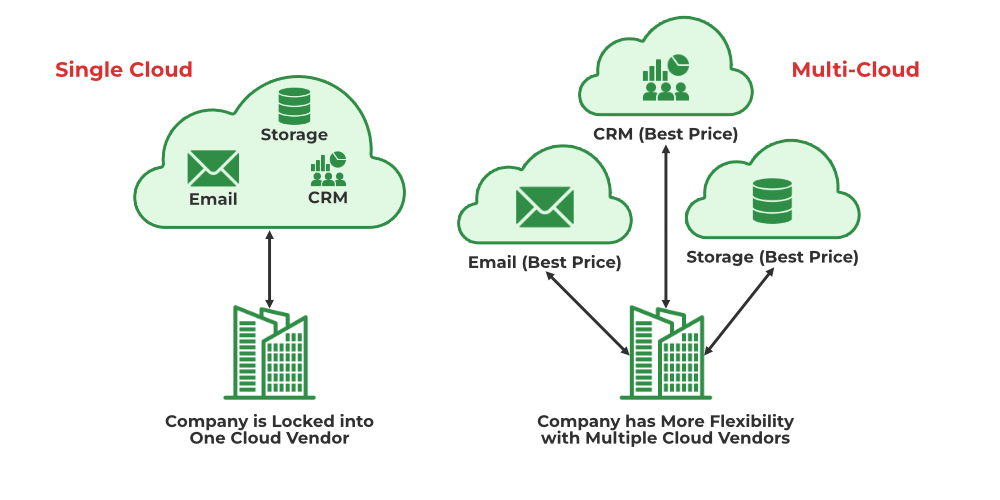
IBM describes cloud computing as having access to physical computing resources such as servers and data storage devices “over the internet with pay-per-use pricing” *(IBM, 2024)*. This is beneficial for an organization like UCB as they can cut costs since they don’t have to invest in the new hardware annually. Each provider specializes in different cloud computing scenarios. AWS (amazon web services) specializes in online servers, but GCP (Google Cloud Platform) is used for online storage. UCB can benefit from using cloud services due to its Speed and Agility. Instead of going back and forth with the IT team and then setting up hardware, they can take advantage of that hardware online instantly *(IBM, 2024).*

To take advantage of the benefits of multiple cloud computing systems, organizations can invest in what’s called “multi-cloud computing”. As mentioned before, different providers specialize in different cloud computing services. These are usually 1 of 3 services:

IaaS – infrastructure as a service

PaaS – Platform as a service

SaaS – Software as a service *(CloudFare, 2024)*

If UCB wanted to use all three, it would be hard to get the best performance by using only one provider. “This is known as Vendor Lock-in” *(GeeksForGeeks, 2023).*

*(Figure 1, Image of how a multi cloud network work. GeeksForGeeks, 2023)*

By taking multiple providers, they ensure peak cloud performance from each provider that is designed for each service. UCB’s would work like this.

Step 1 - Connect to Cloud Providers: They securely connect their on-premises data centre and each cloud provider. This is done by using a Virtual Private Network or VPN

Step 2- Deploy Applications and Data: Next, UCB will decide which cloud service best suits each application and then deploy it. They would need to take factors such as cost and performance into account.

Step3- Manage Network Traffic: Now the network traffic is flowing, it needs to be managed to perform efficiently, this can be done with tools such as load balancers (allows the amount of traffic to customised) as well as other networking tools.

Step4 - Ensure Security: This is one of the most important steps when setting up any network. UCB needs to Implement strong security measures to protect their data and applications. This needs to be done for each cloud environment used.

A diagram of a cloud

Description automatically generatedStep 5- Manage Data Consistency: The data on each cloud service needs to remain the same. To ensure this, UCB needs to create a plan that would make sure each cloud is backed up and replicated frequently.

*(Figure 2, hierarchy diagram for multi cloud platform using Azure, GCP and AWS. Medium, 2024)*

## Blockchain

This is a system that “stores data in blocks which are linked together” *(Investopedia, 2024)*. Once data has been entered into the block, it is difficult to alter, but not impossible. Blockchains have many use cases due to the increased security they offer. Cryptocurrency is the most popular. *(Coursera, 2024)*.Currencies such as bitcoin have all their activity stored on the blockchain. This means transaction amounts as well as sender/receiver info can be seen on the blockchain publicly, acting like a confirmation of payment or “Ledger”. UCB could use blockchain technologies as a database to store information about students and staff.

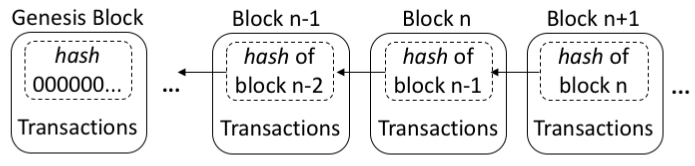
A standard block in a chain contains three pieces of data:

Data – Anything that needs to be stored on the block

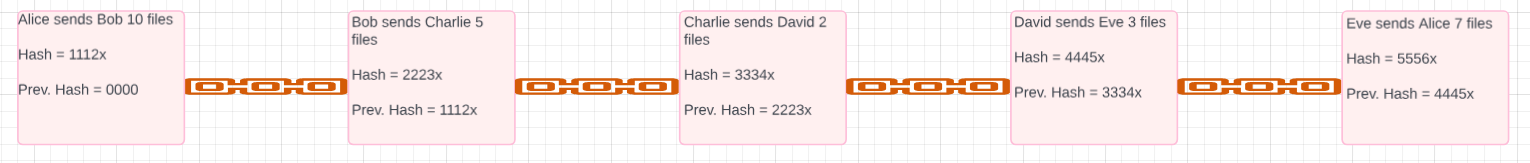
Hash – A “fingerprint” or unique identifier that's calculated for that specific block

Previous Hash – The hash for the prior block in the chain

### Genesis Blocks

Every chain must start with a genesis block. It is a special case in that “it does not reference a previous block” since there is no previous hash to store *(Bitcoin Wiki, 2024).* To reference the Genesis Block, the previous hash on the second block is set to 0. Here is an example:

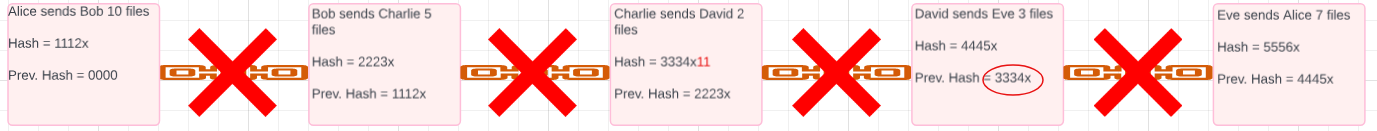
*(Figure 3, example of how a blockchain stores hashes and information. ResearchGate, 2019)*

Here is a blockchain I have created which would suit UCBs use case:

*(figure 4, blockchain designed for UCB use case)*

### Blockchain Tampering

As stated, prior, it's not impossible to alter a blockchain. Once one block in the chain changes, it causes the whole chain to fail. This is done by altering the hash of the individual block. “If a weak hashing system was used to secure the data,” all a hacker would need to do is crack 1 hash and change it *(C-DAC, 2024)*. Here is an example of what this looks like in the UCB blockchain:

The one error in the block hash causes the data integrity to be invalid, meaning what's being stored in the blockchain is not accurate.

## Virtualisation

Sometimes, it can be impractical to run hardware such as servers. Space and price can limit a business on how much data they can store. Virtualisation is a technology that allows users to “create virtual representations of physical machines” *(AWS, 2024)*. With the virtual hardware, the user can run different machines for multiple reasons on a single system. For UCB, virtualisation can be beneficial. Imagine if the IT department stores:

Academic Emails for all students which needs lots of storage

The UCB Portal which needs to be on a separate OS from the Emails

Staff tools such as marking software which only runs on a specific OS

UCB would have to set up three different physical servers for each application, limiting them to the hardware and space available. With virtualisation, they could run multiple VMs with their own memory, processing power, and storage, making their systems more efficient. This is managed by a Hypervisor. A hypervisor is “a software component that manages multiple VMs” in a computer. It also “ensures that each virtual machine gets the allocated resources” *(AWS, 2024).*

### Benefits and Drawbacks of Virtualization

As mentioned before, virtualisation’s main benefit comes from its efficiency. The machines will operate faster and will cost UCB less to run since they don’t have to buy new hardware or pay additional electricity costs. Thought it might be cheaper in the long run, virtualisation does have upfront costs that businesses need to pay. smaller organisations should be prepared to spend “upward of $10,000 for the servers and software licenses.” *(BusinessNewsDaily, 2023)*. This might not affect a bigger company like UCB, but they should be aware that not every system can be virtualised. Some of these systems include databases and anything that requires high amounts of direct user access.

## Current Trends

The best cure for any cyber-attack is a good prevention plan. The Zero Trust model does this perfectly.

### Zero Trust Security Models

As the name suggests, it assumes that “there is an ongoing breach and follows the principle of never trust, always verify,” regardless of whether it is an inside or outside device. *(Cloudflare, 2023)*. This works just like how a login page works when you are new user. 1 key component of Zero Trust is Multi-Factor Authentication or MFA. MFA is simply just a systems’ alternative way of proving that you are authorised user. An example is an email or number to text for a verification code after the password is installed. The benefit of this is that it doesn’t let anyone into your account with a single password. The problem with 2fa is that it is known for locking users out of their accounts. It can ask for a code from a user on an email that they no longer have access to. If that’s the case, they can’t log in anymore. This is important for UCBs IT team since having this model installed would prevent any unauthorised student from entering campuses.

### Biometrics and Behavioural ID

The term biometric technology refers to when we incorporate human features  
into our computer technology. Some examples of this are:

Facial recognition (e.g. Face – ID on Apple devices.)

Fingerprint recognition (e.g. topping up your student account in secondary  
schools).

Heart rate monitors (e.g. heart rate sensors for health purposes.)

Biometric traits are unique, making them difficult to replicate or steal. This provides an advantage over the less safe PIN and Password method. For UCB, biometrics can grant access to Labs, student accounts as well as dorm rooms, “eliminating the need for physical keys.” *(SIA, 2021)*. The problem is they still aren’t 100%. Not all systems can comprehend complex biometrics such as 3D plains, meaning they can be fooled.

Behavioural Authentication focuses on unique patterns of human interactions. It studies how a user “interacts with a device to verify their identity” *(LexisNexis, 2024)*. An example is Keystroke Dynamics. The system will “Analyses the rhythm, speed, and pressure applied to keys during typing” (*MDPI, 2023).* No 2 users would type a password exactly the same way. The system will pick this up. This can also be applied to an examination scenario. If a test is taken online and large amounts of text are written into the field within an inhumane time, the system would also be flagged.

## Challenges

As mentioned prior, the best way to deal with any cyber-attack is to set up a good prevention method. One of the main challenges in today’s industry is that it's usually too late and the attack has already dealt major damage. The best option for a company like UCB would be to have a threat model.

### Dealing with systemic and complex risks

If UCB was suffering from a cyber-attack the best practice would be to adopt the CSIRT or NIST framework. They work as follows:

#### CSIRT

The CSIRT method is a team dedicated to handling any digital/cyber threats an organization might come across. The 3 steps are:

Preparation – prepare a team of staff who have the skills to deal with cyber-attacks as well as security measures they must follow.

Detection – The team uses their resources to detect whether a cyber-attack has occurred or not.

Analysis - the team does further investigations to find out how the attack started and where it came from. They also look for what exactly the attack did to figure out what kind of threat it was (malware, phishing attack etc.)

#### NIST

Detection and Analysis - The threat is both found and analysed in this step, allowing for a less thorough but quicker response time. (NIST, 2019)

Containment, eradication, and recovery – Here, the threat is sectioned off from the system, deleted and all files should be recovered here.

Post-incident activity – UCB is given more liberty to complete any steps of evaluation based on what policies they have in place.

NIST allows for a swifter response to attacks however CSIRT moves the responsibility to an entire team meaning the business can operate smoothly. Overall the NIST technique is best suited for this situation*(CSIRT, 2019)*

### Hybrid Threats

Another challenge many companies face is hackers merging multiple types of cyber-attacks to increase the operational strain on a company trying to recover.

Imagine UCBs attack was a social engineering attempt. The hacker emails a staff member pretending to be a student in need of an emergency password reset. The employee grants the request allowing the hacker into the systems. This is one type of attack. If the hacker went further and held the student’s files for ransom, this would make the attack hybrid *(AmCham, 2022)*. The efforts needed to recover from 2 attacks would cause major issues.

## Impacts

The long-term effect of a cyber-attack can worsen depending on how developed the company is. If UCB did suffer any of the attacks mentioned, the 1st impact they would run into would be economic. The social engineering example showed how the hacker could gain access to student files, but this is low on the scale of what data could have been extracted.

### Economic

This could include student records such as: names address, phone numbers, emails, and birth dates. This also extends to staff records like employee IDs.

UCB would also store payment information from their students which is also vulnerable to theft such as: tuition and fee Payments, credit card numbers, bank account information, payment history, financial aid records and tax returns

### Reputational

An academic establishment like UCB needs to keep a good reputation to attract more students. A known cyber-attack would destroy this. Once their student’s information has been compromised, they will ultimately question how safe their data was initially. This would lead to a loss of customers as students may leave or avoid UCB in fear of data security.

TalkTalk experienced this 1st hand. They fell victim to a data breach in 2015 which resulted in 157,000 user’s financial information being stolen. Many customers also left as they feared for their own account’s safety. TalkTalk wont fully recover from the incident due to the severity of the issue and people still not trusting them. *(ICO, 2021).*

When Sony’s ‘PlayStation Network’ was hacked in 2011, around 77 million accounts were compromised. They took the servers offline temporarily. They then announced a net loss of around $140 Million. This was the greatest loss for a company due to a cyber-attack at the time. UCB is just as vulnerable and could suffer a reduction in profits.

### Legal Consequences

If UCB was attacked, they would even be held accountable. They’d be put to trial where they can face major consequences. Legal impacts also link with other consequences. Costing them even more money, ruining their reputation even more and further slowing down company operations.

Mark Zuckerberg was under fire in 2018 for violating Data Protection Act laws. The situation escalated to a legal battle which he lost. He was ordered to pay over half a million dollars in damages (around 643K).

The Data Protection Act was updated in 2018 and is now under the GDPR (General Data Protection Regulation). They prevent all companies from obtaining user data unlawfully.

(Figure 5, data protection act principles, GOV UK)

Here are a few examples for UCB:

Transparency -UCB must be more specific on what data they obtained from the user. The user must be aware of what individual pieces of information the company is currently storing.

Right to be forgotten - The user now has the right to get the company to forget any previously obtained data

Data Portability - Users can now view the data stored using the 'Transparency Law'. They can claim a digital copy of all the information given in a "commonly used and machine-readable format." *(UKGOV, 2018)*. This is available to see on Facebook, where the user can request an archive of their data.

Graphical user interface, text, application, chat or text message

Description automatically generatedIn 2018 The Computer Misuse Act was passed. It's a law that "criminalizes unauthorized access, modification, or disruption of computer systems and data." *(UKGOV, 2018).* Failure to comply can land you 10 years in prison and hefty fines.

*(figure 6, computer misuse act of 1990)*

# Task 2 - Critically evaluate appropriate tools for developing organisation cyber security systems for businesses of all sizes

## Firewalls

Firewalls Filter incoming and outgoing traffic based on user-set rules. This provides a good layer of security to prevent viruses from automatically sending information to and from your computer system over the internet. the user selects what ports they want to block traffic from. These are the 3 main choices based on the industry standard:

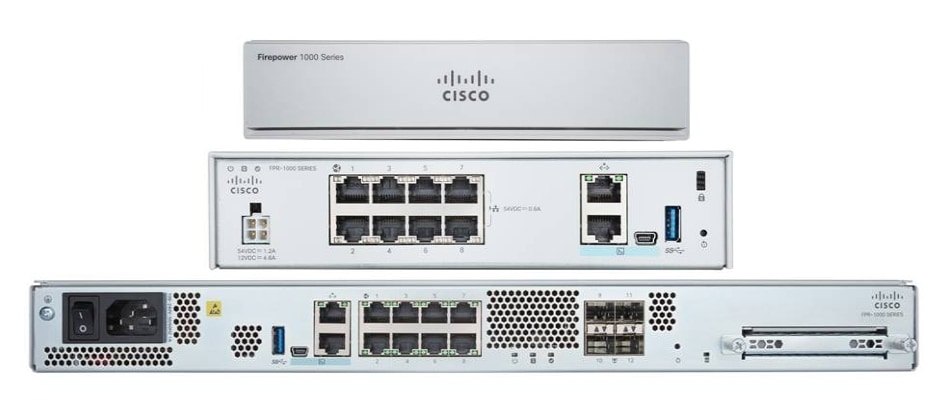
A group of white electronic devices

Description automatically generatedFortinet FortiGate – This antivirus is very popular in the cyber space due to its vast number of features. this includes “advanced threat protection, web filtering, and intrusion prevention” *(Axians, 2024)*. On top of this, it also features multi-layer security which it falls in line with industry standards like NIST Cybersecurity Framework (CSF). The web filtering feature is useful for a company like UCB as they could block unauthorised student traffic on the internet.

*(Figure 7, FortiGate 7000 series firewall. Engage, 2024)*

Palo Alto Network Firewall – Like Fortinet FortiGate, this firewall is recognised for its fleet of tools. Due to its “strong network segmentation, user identity awareness and advanced threat detection”, it is recognised by organisations like CIS Controls and NIST CSF. (*Palo Alto, 2024)* Because of its customisation, Palo Alto does come at a higher cost however an established university like UCB would benefit from investing in it. This would allow more freedom for their IT team to tweak and specify the firewall to their desire.

*(Figure 8, Palo Alto PA-220 Firewall, Radwell, 2024)*

Cisco Firepower Threat Defence – Cisco’s firewall technology is one of the most advanced. It offers “intrusion prevention, malware protection, and advanced threat intelligence” *(Misco, 2024)*. For UCB, they would have to consider the level of technical expertise required to securely set up a firewall. Cisco also offers extra features which aren't included in the standard licence meaning additional costs will occur.

*(Figure 9, Cisco Firepower 1000 series. Cisco, 2024)*

One issue UCB might face is that they’re good at blocking unwanted traffic, but viruses are being engineered with this in mind. They can trick firewalls into allowing their traffic through it.

## Penetration Testing

This is the practice of getting an experienced tester to attempt to find and exploit vulnerabilities in your computer system *(Cloudflare, 2024).* UCB could benefit from this as it would highlight weak areas in their system. The expert is given a form of access. These are:

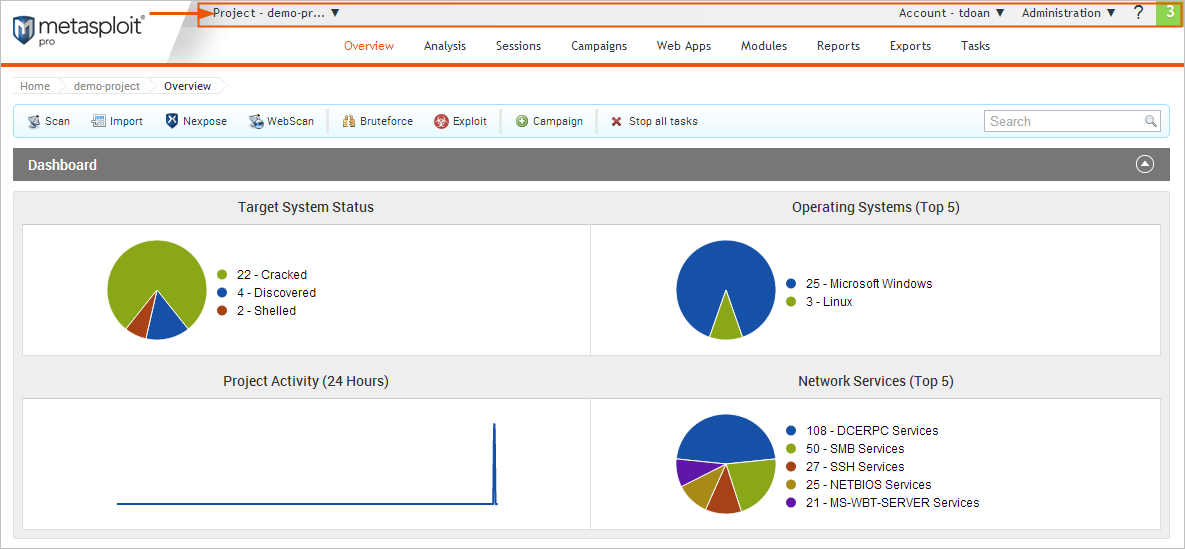
Black Box – The expert is given the bare minimum information to complete the hack

Grey Box – the expert is given minimal information or access to a small amount of the system

White Box – the expert goes in with full access. This is good for mimicking an internal attack

These are 3 of the best Pen Testing tools used in the industry:

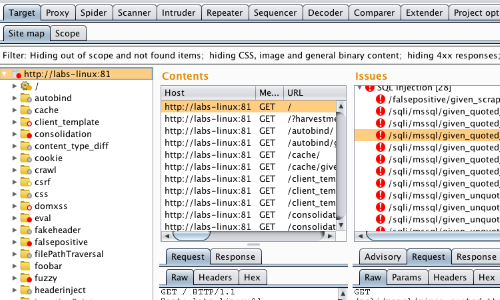
Metasploit Framework - Metasploit is an open-source pen testing tool that lets users use pre-built exploits as well as Create custom ones for specific vulnerabilities. It enables different types of testing by also including post exploitation tools to perform further actions, such as privilege escalation *(Imperva, 2024).* This is a good option for UCB as it has a big community that provides support. IT staff working with the software can easily troubleshoot any errors they encounter; however, its large feature set can be tricky for newer pen testers. It's important UCB hire experienced professionals when using Metasploit.



*(Figure 11, example of Metasploit web UI. DOCS, 2024)*

Kali Linux – If UCB wanted to take a software-based approach, Kali Linux would be their best option. Kali Linux is an Operating System developed for ethical hacking. It comes prepackaged with various hacking tools that allow users to “simulate attacks that target multiple areas of a computer” *(eSecurityPlaent, 2023).* It also offers cyber-forensic tools that the IT team can use to understand how attacks affect systems. This is good for UCB as its user-friendly UI allows for a deeper understanding of the most common attacks UCB is likely to experience

*(Figure 12, Kali Linux GUI. YouTube, 2016)*

BurpSuite – BurpSuite is an online tool used for “testing vulnerabilities in web applications” *(EC-Council, 2024).* It has a host of features such as the ‘intruder’ which lets users launch automatic attacks and the sequencer which lets the tester check how random session tokens are to assess session management security *(Optiv, 2020) (PentestPeople, 2024)*. Apart from its high licence cost and expert knowledge requirement, BurpSuite would be useful for UCB to invest in due to Its automatic features. The staff could simulate multiple different attacks, saving time and effort.

*(Figure 13, BurpSuite, Recon and Analysis)*

# Create a 4-week cyber security industrial plan

To better strengthen UCBs cyber security, its important they undergo a 4-week cyber strengthening plan. The goals of the plan are to create an approach to enhance UCB’s network security and create an increase in awareness in cyber security for their IT staff

## Step 1 - Create a poster to promote cyber security at UCB

A screenshot of a red sign

Description automatically generatedA screenshot of a red screen

Description automatically generated

## Step 2 – Create a Phishing Prevention email

A screenshot of a computer

Description automatically generatedTo get a broader reach for cyber security, The UCB staff should create an email that briefly details what phishing attacks are and how to spot them. This will help the less technical lecturers understand how to be safe online.

## Step 3 – Importance of MFA implementation in the staff members

A green and black poster with text and a lock

Description automatically generatedTo show the importance of multi factor authentication. The staff should create a post for UCB’s social media accounts. Social media hacks are becoming more prevalent on people who only use their password to protect themselves. This is a good platform for UCB to address this.

## Step 4 – An email on how to protect staff from further threats

A screenshot of a computer

Description automatically generatedAs a follow up for the 1st week’s email, I also included further methods for IT and general staff at UCB to spot alternative attacks. Threats like phishing are the most important attacks UCB need to prevent as they rely on social compliance. One mistake from one staff member can create a vulnerability in UCB’s system, allowing for unauthorised access.

# Conclusion

In Conclusion, cloud computing (CC) can be used to access computing resources over the internet without expensive hardware. CC providers specialise in different areas: infrastructure, platform, and software as a service. Companies can use all three to take advantage of the best services. This is called Multi Cloud Computing. Another CC feature is virtualisation. UCB could use this to run multiple specific computers from one machine. Its efficient but has a high upfront cost. Another emerging trend is blockchains. They store data in ‘blocks’ like a record. They feature a first (genesis) block, a hash, and a previous hash. The genesis block doesn’t have a previous hash. Blockchain tampering is where a user maliciously enters an incorrect hash in one of the blocks which causes the whole chain to be invalid.

UCB’s prevention plan can benefit from 2 tools. the first one is a Zero Trust Security Model. Its treats everyone like a new user who needs to re-verify authenticity. It uses MFA or multi factor authentication, MFA requires a second or even 3rd login method for users. The second tool is Biometrics. Features such as fingerprints and irises aren’t shared between people, making biometric scanners good for identifying staff. If UCB does suffer from a more advanced attack, it would be optimal to adopt either the NIST or CSIRT framework. They both work similarly by laying out a plan for UCB. They prepare to detect the attack, execute the defence, and then analyse and complete a post attack procedure. This is also useful for ‘Hybrid Threats’. This is when hackers combine multiple attacks to gain unauthorised access. Causing more damage. An attack on UCB could cause economical damage as student financial information might get leaked. they would also receive reputational damage to their name and even legal consequences if the damage was severe enough.

For any business a firewall is essential. Companies like Cisco, Palo Alto and Fortinet have industry standard hardware to defend a network. In terms of Penetration Testing (private exploit hunting), UCB should look at Metasploit, Kali Linux OS and Burp Suite. This should go alongside a for week plan to improve security. Using social media and staff emails, UCB can bring more awareness to cyber security tech such as MFA and Phishing.

*End of Assignment*

anjalibo6rb0 (2023). *Vendor Lock-in in Cloud Computing*. [online] GeeksforGeeks. Available at: https://www.geeksforgeeks.org/vendor-lock-in-in-cloud-computing/.

AWS (2024). *What Is Virtualization? - Cloud Computing Virtualization - AWS*. [online] Amazon Web Services, Inc. Available at: https://aws.amazon.com/what-is/virtualization/.

Axians (2024). *Glossary - What is FortiGate Firewall? | Axians UK*. [online] Axians UK. Available at: https://www.axians.co.uk/glossary/what-is-fortigate-firewall/.

Bank Of America (2020). *Cyber Attack Protection for Schools & Universities*. [online] Bank of America. Available at: https://business.bofa.com/en-us/content/cyber-attack-protection-for-universities.html.

C-DAC. (n.d.). *Blockchain Explained - Concept, Function and Security*. [online] Available at: https://www.cdac.in/index.aspx?id=print\_page&print=blog\_blockchain\_exp\_CFS.

Cichonski, P., Millar, T., Grance, T. and Scarfone, K. (2012). Computer security incident handling guide. *Computer Security Incident Handling Guide*, [online] 2(2). doi:https://doi.org/10.6028/nist.sp.800-61r2.

CloudFare (2024). *What is multi-cloud? | Multi-cloud definition*. [online] Cloudflare.com. Available at: https://www.cloudflare.com/en-gb/learning/cloud/what-is-multicloud/.

Cloudflare (2023). Zero Trust Security | What’s a Zero Trust Network? | Cloudflare UK. *Cloudflare*. [online] Available at: https://www.cloudflare.com/en-gb/learning/security/glossary/what-is-zero-trust/.

Cloudflare (2024). What Is Penetration Testing? What Is Pen Testing? | Cloudflare UK. *Cloudflare*. [online] Available at: https://www.cloudflare.com/en-gb/learning/security/glossary/what-is-penetration-testing/.

Coursera Staff (2023). *Blockchain in Cryptocurrency: Beginner Guide and Career Outlook*. [online] Coursera. Available at: https://www.coursera.org/articles/blockchain-cryptocurrency.

CSIRT (2024). *CSIRT, Computer Security Incident Response Team*. [online] www.csirt.org. Available at: https://www.csirt.org/.

de Oliveira, M.T. (2019). *Schematic view of the data structure of a blockchain.* *https://www.researchgate.net/figure/Schematic-view-of-the-data-structure-of-a-blockchain-The-genesis-block-represents-the\_fig1\_332379108*.

EC-Council (2024). *Burp Suite for Penetration Testing of Web Applications | EC-Council*. [online] Cybersecurity Exchange. Available at: https://www.eccouncil.org/cybersecurity-exchange/penetration-testing/burp-suite-penetration-testing-web-application/.

Fingerprints, M.P. (2021). *The Key to Modern Access Control: How Biometric Solutions Can Offer Both Security and Convenience*. [online] Security Industry Association. Available at: https://www.securityindustry.org/2021/07/27/the-key-to-modern-access-control-how-biometric-solutions-can-offer-both-security-and-convenience/.

GeeksForGeeks (2023). *Image of how a multi cloud network work*. *https://www.geeksforgeeks.org/vendor-lock-in-in-cloud-computing/*.

Giri, B. (2024). *hierarchy diagram for multi cloud platform using microsoft azure, Google cloud and AWS*. *https://miro.medium.com/v2/resize:fit:720/format:webp/1\*qf9l3V\_3wYiIaFSHvXatag.png*.

GOV.UK (2018). *Data Protection Act*. [online] GOV.UK. Available at: https://www.gov.uk/data-protection.

Hayes, A. (2024). *Blockchain Facts: What Is It, How It Works, and How It Can Be Used*. [online] Investopedia. Available at: https://www.investopedia.com/terms/b/blockchain.asp.

ICO (2021). *TalkTalk Cyber Attack – How the ICO’s Investigation Unfolded*. [online] ico.org.uk. Available at: https://ico.org.uk/about-the-ico/media-centre/talktalk-cyber-attack-how-the-ico-investigation-unfolded/.

Imperva (2024). *What Is Metasploit | Tools & Components Explained | Imperva*. [online] Learning Center. Available at: https://www.imperva.com/learn/application-security/metasploit/.

LexisNexis (n.d.). *What is Behavioral Biometrics*. [online] LexisNexis Risk Solutions. Available at: https://risk.lexisnexis.com/global/en/insights-resources/article/what-is-behavioral-biometrics.

Maury, J. (2023). *Kali Linux Penetration Testing Tutorial: Step-By-Step Process*. [online] eSecurityPlanet. Available at: https://www.esecurityplanet.com/networks/kali-linux-tutorial/.

Multiple Contributors (2009). *Genesis block - Bitcoin Wiki*. [online] Bitcoin.it. Available at: https://en.bitcoin.it/wiki/Genesis\_block.

Najwa Altwaijry (2023). Authentication by Keystroke Dynamics: The Influence of Typing Language. *Applied Sciences*, [online] 13(20), pp.11478–11478. doi:https://doi.org/10.3390/app132011478.

Nickel, A. (2022). *Hybrid War – Cyber attacks – AMCHAM*. [online] Amcham.lu. Available at: https://www.amcham.lu/newsletter/hybrid-war-cyber-attacks/ [Accessed 1 Nov. 2024].

Palo Alto (2024). *Policy Object: Applications*. [online] Paloaltonetworks.com. Available at: https://docs.paloaltonetworks.com/network-security/security-policy/administration/objects/applications [Accessed 9 Nov. 2024].

Part number (2024). *Cisco FirePOWER Threat Defense, Malware and URL - Subscription licence*. [online] Misco.co.uk. Available at: https://www.misco.co.uk/product/Software/Miscellaneous/Cisco/L-FPR1120T-TMC-1Y-Cisco-FirePOWER-Threat-Defense-Malware-and-URL---?prodid=5213097 [Accessed 9 Nov. 2024].

Pentest People (2024). *A Quick Burp Suite Sequencer Lab*. [online] Pentestpeople.com. Available at: https://www.pentestpeople.com/blog-posts/a-quick-burp-suite-sequencer-lab [Accessed 17 Nov. 2024].

Rivera, A. (2023). *The Pros and Cons of Virtualization*. [online] Business News Daily. Available at: https://www.businessnewsdaily.com/6014-pros-cons-virtualization.html.

S, J. (2023). *Fortinet Fortigate Firewalls*. [online] Nexigen. Available at: https://www.nexigen.com/cyber-security/fortinet-fortigate-firewalls-everything-you-need-to-know/.

Subramanya, S. (2020). *Brute Force Account Testing Using Burp Intruder*. [online] Optiv. Available at: https://optiv.com/insights/source-zero/blog/brute-force-account-testing-using-burp-intruder [Accessed 17 Nov. 2024].

Susnjara, S. and Smalley, I. (2024a). *What is cloud computing?* [online] www.ibm.com. Available at: https://www.ibm.com/topics/cloud-computing.

Susnjara, S. and Smalley, I. (2024b). *What is cloud computing?* [online] www.ibm.com. Available at: https://www.ibm.com/topics/cloud-computing.