REPORT

Group name and candidates: Group 2 Ahmed Anwar – ahmedan@uia.no

Course code	IS-214
Course name	Information Systems Security
Course responsible	Wael Anwar Abdel Aziz Soliman
Deadline	28.04.2025 // 23:59
Number of words (whole document)	4372 words
Project/product title	Individual Creative Writing

We confirm that we do not cite or otherwise use other people's work without this being stated and that all references are listed.	**Yes** **X**	**No**

Can the report be used for teaching purposes?	**Yes** **X**	**No**

We confirm that everyone in the group has contributed to the report	**Yes** **X**	**No**

Table of Contents

Part 1: The Context

1.1 The Company

When choosing and analyzing a cybersecurity incident, the first logical step is to describe the company/victim. In this case, which is a real-life incident, the company/victim is Yussouf & Co – Charted Accountants.

Yussouf & Co are a leading firm of charted accountants, tax and business advisors based in North-West London. The company is also a member firm of the Institute of Charted Accountants in England and Wales (ICAEW). According to themselves "A primary goal of a charted accountant is to prepare and analyze financial statements, ensuring they comply with relevant accounting standards and regulations." (Yussouf & Co, 2023). The company provides a variety of services in different fields such as Business Startup, Accountancy, Taxation, Payroll, HMRC Investigations and Business Advisory.

When it comes to assets, we can first preface by saying assets are anything of value for the company or organization. On the other hand, informational assets are anything that possesses or processes valuable organizational information.

We can begin by identifying the physical assets of the company which would include the office spaces, computers used at each cubicle and the server which manages the network resources. On the other hand, we have informational assets which includes **Financial records** of every client including bank statements & employee details, **Client reports** detailing financial strategies and plans, **HMRC communications** handling tax investigations and regulations, **Taxation information** and **Payroll information** which ensures clients comply with tax & payroll laws and regulations, different schemes, etc. Alongside Client data, another asset is the **Company data** which includes internal files and reports of the company.

1.2 The Environment

The next step in analyzing a cybersecurity incident, is exploring the environment in which the company exists in. This also includes exploring common threats that may appear, value they may obtain and possible attack motivations

When it comes to the environment, the company is a relatively small company operating out of the big 4 accounting firms which includes Deloitte, KMPG, PwC and EY. This also reflects the personnel, with only 7 employees working at company and 1 IT-specialist working on a freelancer basis.

The common threats faced by the company and similar companies within the same industry is cybersecurity threats due to outdated technology and digital architecture. Especially when it comes to the smaller accounting firms outside of the big 4, there is just not enough resources to address every issue or even instate an internal IT department.

Common assets and value attached to the company and environment includes tangible assets which are the physical resources at hand, information assets which are confidential with

things such as financial records, personal information, reports and personnel which includes charted accountants and tax professionals.

When it comes to attack motivation, one point of view can be that the company is easier to target and breach as it's a smaller accounting firm. This means the company doesn't have the resources of a Deloitte or a PwC to have their own IT department or to have an updated and modern IT infrastructure. With smaller companies, there are small cracks and areas of vulnerabilities hackers can see as a good opportunity weighing the risks against the rewards.

1.3 The Attacker

Now it is time to discuss the attacker in this given situation, which is the Lockbit Ransomware Group. LockBit is a cybercriminal group who follow a ransomware as a service (RaaS) approach. The group has been active since 2019 and have been notorious for being the most prolific group in the field of cyberattacks. How the group operates is buy selling their services to cybercriminals, who target organizations and companies, deploying LockBit ransomware.

It is to be believed the LockBit group had no political motivation to any of the attacks, which leads people to believe the reasoning was all monetary. Their Website on the dark web, would share the recent attacks on their victims and leak the data from those who did not pay the ransom.

According to Flashpoint, "LockBit accounted for 30.25% of all known ransomware attacks from August 2021 to August 2022." (Flashpoint, 2023). Another interesting statistic is that "80.5 percent of LockBit victims are small and medium-size businesses" (Flashpoint, 2023).

The Lockbit Ransomware Group would be classed as 'The Crooks' as there was clear motivation through financial gains, operations was run through the dark web, and also with the group being under the sub-group 'malware developers' which are key players within 'The Crooks'.

1.4 The Attack

We can now begin by exploring the attack done by the Lockbit Ransomware Group on the victim Yussouf & Co. The type of attack was a ransomware attack which was conducted in July 2022. Ransomware is a type of software that allows hackers to gain access to confidential information on the victim's computing environment.

This was an active and syntactic attack which occurred through the act of phishing. Phishing is a type of attack which uses fraudulent emails, text messages or phone calls which trick people into giving access to sensitive data (Kosinski, 2024). The attack can also be seen as both external and internal, as the attack was initiated from the outside through the hackers sending an email but also initiated from an insider (the secretary) accessing the email.

The attacker sent an email to the company, where at the office the secretary clicked on the email and allowed the software to attach itself to the server which happened on the Thursday/Friday. The following Monday, the employees noticed something was wrong and

later met a screen on the secretary's computer demanding a ransom to give back the access of the files and data, but also to not leak the data.

This lead to the company informing their IT specialist to come and see what should be done next. This led to them wiping and disconnecting the computer from the server and later wiping the server data. This meant they had to restore the back leaving the company to lose maybe one/two days of work. The result was ultimately the company ignoring the ransom demand and wiping the server. To this day, it is still unsure if the data the hackers had access to was uploaded to their website on the dark web or not.

Part 2: Think For Yourself

2.1 Reflection

The first sub-part of 'Part 2: Think for Yourself' consists of reflecting over the incident from the perspective of the individual responsible for the cybersecurity of the company. This includes looking at the different aspects that are apparent within the information systems security, reflecting over how incident could be handled better and categorizing the extent of the incident.

2.1.1 Aspects of the information systems security

Technical Aspects

We can first take into account the technical aspects of the information systems security in the company that allowed the attack to take place. The first technical aspect allowing the attack to take place would be the company's email filtering system - or more so, the lack of it. Due to the nonexistent filtering system, the phishing email reached the secretary which led to the attack taking place. Email filtering is a method/solution which involves sorting and identifying emails which are deemed to be spam, non-productive or malicious (Darktrace, n.d.).

The next technical aspect allowing for the attack is the lack of security monitoring. When looking back at the incident, it was only until the Monday when the employees found out about the attack. If there was monitoring system implemented, the attack would have been noticed earlier minimizing or avoiding the impact of the attack. Cybersecurity monitoring is the process of tracking and analyzing systems to detect and respond to threats. Examples of tools/services includes SIEM tools, IDS/IPS tools and EDR solutions (Keepnet Labs, 2024).

Another technical aspect allowing for the attack to take place would be the anti-virus software. Looking back at the situation and context, we can see that the accounting firm was operating on a free anti-virus software due to resource restriction and negligence in priority. Although the free AVG anti-virus has its advantages for the price you get, it has many limitations lacking many advanced features and functions (Livingston, 2023).

The last notable technical aspect would be the lack of Multi-Factor Authentication. This would useful as the attacker gained access to confidential files and data which could have been stopped through MFA which demands a second authentication factor and denies

unauthorized access. This use of MFA is as specially important as it defends against phishing requiring additional verification factors (Ibrahim, 2024).

Formal Aspects

In the case of formal aspects of the information systems security that allowed the attack to take place, we have to reflect over the laws, regulations and policies that were neglected or implemented wrongly. The potential of these laws, regulations and policies, which are listed below, could have helped the company be more security conscious, better prepared for any potential attacks and respond in a more efficient manner.

The first formal aspect is related to UK GDPR (General Data Protection Regulation) which applies to UK-based businesses and organizations concerning the processing of personal data (ICO, 2023). The UK GDPR requires business and organizations to implement a good amount of security precautions for the purpose of protecting personal data. If the company had stronger security measures in place, the attack may be minimized or even prevented. The regulation also promotes regular and thorough security training, which would definitely have influenced the behavior and actions of the secretary who received the phishing email.

The other notable formal aspect is the UK certification scheme 'Cyber Essentials'. Cyber Essentials is a government backed certification scheme which helps ensuring organization's and companies' customers and own data are kept safe from cyberattacks. Cyber Essentials helps organizations and businesses ensures technical controls are in place such as user access control, malware protection, security update management and firewalls which would helped the company be better prepared and equipped for the attack and incident that took place (National Cyber Security Centre, 2023). If the company had obtained the certification from Cyber Essentials, they would also be required to implement an email filtering system which would decrease the risk of phishing attacks (National Cyber Security Centre, 2018).

Informal Aspects

The informal aspects apparent within information systems security which allowed the attack to happen would mainly be the culture and lack of knowledge from the company and its employees.

With the company being relatively small and close-knitted having the same employees for a prolonged period of time, the culture of the company could have been stagnant and not forward-thinking resulting into falling behind when it comes to being cyber aware in this new digital world. The lack of new and fresh minds from an IT perspective led to the company obtaining a weak digital security culture which led to them not realizing the importance of prioritizing security.

The other aspect is the lack of knowledge from its employees which, when looking back, was the ultimate reason for the attack to take place. The negligence of possible threats from employees derives from the lack of training and workshops being available.

2.1.2 How could the incident be handled better

When reflecting over could the incident be handled better and how personally I would handle such as situation, we must look over the key actions which were done and explore if there other alternatives more beneficial to the company and overall incident.

For the most part, I believe the incident was handled to the best of its ability taking into account the resources available and the damage that had already been inflicted. Some areas including communication was performed correctly through notifying every client about the incident that took place and reporting to the authorities to get further instructions. However, there are other areas in which the incident could have been handled better and what I personally would have done coming from the perspective of the induvial responsible for the cybersecurity of the company.

One area for improvement which we can first explore is preserving evidence and more specifically, digital forensics. In order to protect the interests of the company and assist the authorities in an investigation, the company must determine the 'whats and hows' of the incident which is also referred to as digital forensics (Whitman & Mattord, 2022, p. 200). Digital forensics involves the "preservation, identification, extraction, documentation, and interpretation" of computer media for analysis, following clear methodology (Whitman & Mattord, 2022, p.200). In our case, instead of immediately wiping the server clean removing valuable forensic data which would have helped further understand the attack, the company should have quarantined the server which would have allowed for a forensic analysis to take place.

Another area of improvement which could be explored in doing differently would be how the company monitored the incident post-attack. As mentioned before, the company are still unsure if any of the compromised data had been leaked on Lockbit's dark web leak site due to the company ignoring the ransom and not negotiating with the hackers. Instead of just notifying the clients about the attack and telling them to inform the company if they notice anything out of the norm, I would have implemented a few different steps to really investigate what the true impact of the attack really was.

The first thing I would do is monitor Lockbit's dark web leak site to find if the data compromised was actually leaked. Implementing a dark web monitoring service would be beneficial in a situation like this. Another thing I would do would be to investigate and monitor identity theft cases relating to clients and employees connected to the company. Due to there being financial assets and data which was involved in the attack, it would be logical to check unusual bank activity or new registrations of fake emails and company names impersonating the company trying to trick new potential victims.

2.1.3 Categorizing the incident

Categorizing the incident based on the impact, using the scale which consist of 'insignificant, minor, moderate, major or catastrophic', the verdict would ultimately land on minor. This is due to the company not paying the ransom and ultimately wiping the server data. Due to poor backups, the company only lost one to two days of work, which made for a really easy

recovery process. When it comes to reputation, the credibility of the company was not affected due to the company's transparency when it came to discussing the attack with their clients but also the loyalty the company had with their clients.

2.2 Implementation

The second sub-part of 'Part 2: Think for Yourself' consists of implementing different methods and steps in order to ensure the security of the company, as the person responsible for the information security of the company. This includes exploring potential prevention, mitigation and recovery methods while also highlighting which of the following methods and steps would be considered most critical.

2.2.1 Implementing prevention, mitigation and recovery methods

Prevention methods

We can first begin by delving into implementing various prevention methods in order to stop future attacks from occurring. The first method worth exploring to implement would be security awareness training and courses. As a prevention measure, ingraining a new culture within the workplace of security awareness and zero trust will help aid in minimizing human error and building an environment where colleagues feel confident and safe in reporting suspicious activity. I would first conduct a general security awareness workshop for all employees to attend and would later conduct a phishing awareness training course in direct response to the attack. This would cover and inform social engineering tactics and email security. In addition to the security awareness training and courses, it is important to keep up the culture and new initiative making the topic cybersecurity fresh in the minds of the employees. For that reason, I would also implement phishing simulation tests that would be sent to employees which can later be reviewed showing how many failed or clicked the 'suspicious email' which could indicate for further/less training.

The next method worth exploring to implement would be an investment in email filtering and anti-phishing solution. As a prevention measure, the newly implemented solution would stop irrelevant and suspicious activity from ever reaching the 'front door' of the company. I would implement Microsoft Defender as it protects against malware, phishing and BECs through using AI to detect possible threats and suspicious activity. Implementation wise, Microsoft Defender is relatively easy to implement, with it being integrated into Microsoft 365. Policies can also be defined and set up through Microsoft's 365 Security & Compliance Center (Microsoft Learn, 2023). The reasoning behind setting up an email filtering and ant-phishing solution/tool is due to the lack of an email filtering system allowing for the attack to happen.

Mitigation methods

We can now explore the various mitigation methods that I would implement to reduce the impact of the attack or other possible attacks in real life time. The first method to be implemented is a monitoring system. As mentioned before, SIEM (Security Information & Event Management) tool would be ideal to deploy collecting logs and analyzing security events allowing the company to be updated 24/7, increasing incident response time (Fortinet, n.d.). One specific solution offered by Splunk is a Cloud based SIEM solution which

scalability-wise handle the transition of the company quite easily with the addition of it being flexible to monitor and manage (Kidd, 2023).

The next mitigation method that I would implement is an incident response (IR) plan. The incident response plan is the documented product of incident response planning. The documented product is in the form of a plan which reflects the organization's intended actions in the event of an incident (Whitman & Mattord, 2022, p. 186). Having a plan in place for such crises can help mitigate the incident and soften the impact of an attack. It is important to note that within an incident response plan, the roles and responsibilities within the company should be clearly defined alongside an alert roster, which lists important figures within the organization emergency that should be contacted during the course of an incident. According to NIST SP 800-61, an incident response plan should include: The organization's mission, strategies, approaches, goals, senior management approval, how the IR team will communicate with others in the organization, roadmap, and metrics for evaluation (Whitman & Mattord, 2022, p. 188). It is important to note when implementing a new initiative/plan like this one, communication to the employees is critical. If the employees understand why these changes are being implemented, the likelihood for integrating the initiative/plan increases.

Another notable method to implement would be Identity & Access Management (IAM). This ultimately concerns establishing a role-based access control and the inclusion of MFA. IAM is a solution towards controlling what users can and can't access so that sensitive information are only with the people that need to work with them which reduces unnecessary access within the workplace. The need for secure access goes beyond employees including clients, contractors and people working on personal devices. The positives include the right access for the right people, protection and data encryption and efficient collaboration (Microsoft, 2024).

The first part is Identity Management, which checks a login attempt against a database which includes records over access levels and permissions for each individual. Access Management is the second part which keeps tracks over the resources each induvial has permission to access. When it comes to implementing, planning is essential for a successful impact within the company and is important to map out the different roles and figures that are present for creating the architecture of the IAM system. Microsoft Entra was a reliable solution I found, which would fit the casual and easy implementation the company would require. (Microsoft, 2024).

Recovery methods

Finally, we can now explore the chosen recovery methods that I would implement as the induvial responsible for the security of the company. The first method would involve forensic analysis. Digital Forensics is "Investigations that involve the preservation, identification, extraction, documentation, and interpretation of computer media for evidentiary and root cause analysis, following clear, well-defined methods." (Whitman & Mattord, 2022, p. 200). The key part of this definition is preservation, identification and interpretation which I felt was something the company lacked during the incident and would benefit greatly from after implementation. The company didn't get a chance to actually figure out what really happened in terms of the attack due to them wiping the server which limited how they reflected over the

incident or decided which areas to strength. Digital Forensics allows for that to happen, painting a clear picture of the 'crime scene' pointing to areas of weakness and root causes of an attack.

The other recovery method I would implement is a disaster recovery (DR) plan. The DR plan focuses on restoring operations within an organization in the event of an incident or crisis. The DR plan document will consist of detailed guidelines and procedures for restoring a damaged system depending on the circumstances and context of the incident (Whitman & Mattord, 2022, p. 208). As mentioned before, It is important to communicate with the employees and management of the company on why these new plans and initiatives are being enforced through workshops and meetings. This way, the plans can be accepted by the company and workplace, and be followed and respected leading to a more secure and well-prepared environment. It is also important to note that testing the plan and performing training and exercise with employees will increase plan effectiveness and overall preparations (Whitman & Mattord, 2022, p. 212).

2.2.2 Most critical methods and steps

We can now reflect over the most critical methods and steps concerning the company and their overall security. When exploring the most critical methods and steps mentioned above, we must take into account cost effectiveness, the priority of the method (is it a must?) and the consequences of implementing such methods or steps such as performance or workflow drawbacks.

Security awareness training courses would transform the culture of the company creating a safe and aware environment including better informed employees. The method is not the costliest and can have huge positive impacts on the company and its employees making it a critical step/method to take for the future of the company. While an email filtering and anti-phishing system is on the more expensive side, its benefits are huge with it potential blocking out irrelevant emails and possible threats and suspicious activity leading to a boost in performance by employees who have less distractions.

An identity and access management solution like Microsoft Entra is also a critical step to implement as it protects and limits access to sensitive and confidential information. While implementing an IAM solution may be costly, the benefits are clear too see with control over access and security within the company. Creating levels of access between management and employees will also boost performance in terms of structuring the workload and limiting possible distractions.

A DR plan can surely be beneficial in guiding the company to survive and restore operations in the event of an incident. On the other hand, it drawbacks do include relatively frequent updates and adjustments to the plan demanding resources like time and effort, which in my opinion is worth it for the stability and future prosperity of the company.

In the case of the company Yussouf & Co, operating as a small company with limited resources, they must work smart in keeping the company as safe as possible with the methods and steps that both align with their work environment and capacity. Changing the culture is a

must in terms of the safety of the company and their assets. Though some of the tools and solutions which are mentioned above are critical to include, others can be seen as the cherry on top of a solid foundation.

References

Darktrace. (n.d.). *What is Email Filtering? Definition & Examples*. Retrieved 15.03.2025 from: https://darktrace.com/cyber-ai-glossary/email-filtering

Flashpoint. (2023, July 20). *LockBit Ransomware: Inside the World's Most Active Ransomware Group*. Retrieved 01.03.2025 from: https://flashpoint.io/blog/lockbit/

Fortinet. (n.d.). *What is SIEM: A security information and event management primer*. Retrieved 09.04.2025 from: https://www.fortinet.com/resources/cyberglossary/what-is-siem

Ibrahim, M. (2024, August 5). *The Multifaceted Benefits of Multi-Factor Authentication*. SuperTokens. Retrieved 18.03.2025 from: https://supertokens.com/blog/benefits-of-multi-factor-authentication

ICO. (2023, May 19). *The UK GDPR*. Retrieved 22.03.2025 from: https://ico.org.uk/for-organisations/data-protection-and-the-eu/data-protection-and-the-eu-in-detail/the-uk-gdpr/

Keepnet Labs. (2024, December 25). *What is Monitoring in Cybersecurity and Why is it Important?* Retrieved 16.03.2025 from: https://keepnetlabs.com/blog/what-is-monitoring-in-cybersecurity-and-why-is-it-important

Kidd, C. (2023, October 12). *What's SIEM? Security Information & Event Management Explained*. Splunk. Retrieved 09.04.2025 from: https://www.splunk.com/en_us/blog/learn/siem-security-information-event-management.html

Kosinski, M. (2024, May 17). *Phishing*. IBM. Retrieved 02.03.2025 from: https://www.ibm.com/think/topics/phishing

Livingston, Z. (2023, August 26). *AVG Antivirus Review: Features, Pricing & More*. Forbes Advisor. Retrieved 18.03.2025 from: https://www.forbes.com/advisor/business/software/avg-antivirus-review/

Microsoft. (2024). *What is Identity Access Management (IAM)?* Microsoft Security. Retrieved 09.04.2025 from: https://www.microsoft.com/en-us/security/business/security-101/what-is-identity-access-management-iam

Microsoft Learn. (2023, December 7). *Microsoft Defender for Office 365 service description - Service Descriptions*. Learn.microsoft.com. Retrieved 07.04.2025 from: https://learn.microsoft.com/en-us/office365/servicedescriptions/office-365-advanced-threat-protection-service-description

National Cyber Security Centre. (2018, February 5). *Phishing attacks: defending your organisation*. NCSC.gov.uk. Retrieved 22.03.2025 from: https://www.ncsc.gov.uk/guidance/phishing

National Cyber Security Centre. (2023). *About Cyber Essentials*. NCSC.gov.uk. Retrieved 22.03.2025 from: https://www.ncsc.gov.uk/cyberessentials/overview

Whitman, M. E., & Mattord, H. J. (2022). *Principles Of Information Security.* (7th ed.). Cengage Learning Custom P.

Yussouf & Co. (2023). *About Us*. yussouf.co.uk. Retrieved 23.02.2025 from: https://www.yussouf.co.uk/about-us/