Organizational Systems Security

Assignment 2

Unit 7

George Hotten

Task 1

Disaster Recovery Policies

A DRP is a plan that should be taken in the event of a disaster. This could be because of a human error or because of natural disasters. This can include moving to a different location (e.g., moving office), restoring backup data or hiring equipment

Updating of Security Procedures

The security procedures should be regularly updated to keep the system safe from the latest threats by blocking threats as the occur or stopping them from ever happening

Security Audits

Checks on the security should be done regularly to ensure the policy is being followed properly. This should be as often as possible to ensure all systems are safe

Codes of Conduct

This makes sure everyone in the organisations uses all the provided services. For example, policy for using emails, the internet, and software installation. All network users should sign to show their agreement of the policy.

Surveillance Policies

CCTV can be controversial among workers as it can often cause them distress. The areas monitored by CCTV should be agreed with and the reasons for the surveillance should be outlined clearly.

Risk Management

This should be carried out to identify any risks that may occur and how likely they are. There should be methods put in place to prevent these risks from happening to keep the workers safe.

Budget Setting

Organisations should have a set budge on how much they will spend on security and disaster recovery. This would cover backup storage, separate office, etc.

Task 2

Hiring Policies

A hiring policy is the checks that must be done to ensure the employee is right for the job. This includes running background checks (e.g., checking social media, qualifications, credit score), previous employment checks (e.g., experience, how they left the previous job, any other personal info), references (e.g., their work ethic, attitude, professionalism), and criminal records checks.

This can affect security as if someone who was previous known for leaking confidential information and breaking policies is hired, they could do the same for this company which could be a threat to the company as their private information could be leaked.

Separation of Duties

Separation of duties is the splitting of tasks between multiple employees to ensure that all workloads are manageable. However, it must ensure if a staff member isn’t present, work can continue without being caught up on their absence.

This can affect security as if a staff member isn't present and someone has to cover their work, if not properly trained they could do something they're not supposed to and end up harming a company service (for example taking a network offline) or accidently create a security vulnerability.

Disciplinary Procedures

Disciplinary procedures are used to handle any misconduct or inappropriate behaviour in the workplace. This ensures staff follow the agreements of their organisation and act in a good manor. Failure to comply could result in verbal warnings, written warnings and potentially termination of employment.

This affects security as if staff are not properly punished for their misbehaviours, they are more likely to do it again and continue to breach the company's policies which could end up being a security risk to them.

Training and communicating with staff

This ensures that staff are properly trained for the job they are in and know all the proper procedures. This includes knowing what is expected of them, first aid, fire safety, etc. This ensures they know what to do in different scenarios and are properly trained to do the

If staff are not properly trained, they could do actions that break the company's policy which could end up putting the company at risk as they aren't following the proper policies.

Task 3

Computer Misuse Act

This act ensures that if your services are hacked, you can take legal action on the people responsible. It covers the unauthorized access of:

- Computer programs or data
- Services with the intent to commit further offences
- Modifications of computer material

This helps deter cybercriminals as they can be legally punished for their actions, and it also ensures that the company can get justice for any damages they suffer.

Copyright, Designs and Patents Act

This act protects the work you have created. For example, work such as code, music, writing, and arts are all protected under this law. The content of websites is also protected under copyright. For example, the company's website and any digital material they create can be licensed and protected from anyone attempting to steal their work.

Data Protection Act

This act governs how companies must store and protect sensitive data. This applies to paper and electronically stored data. The 8 acts are:

- Fair and lawful
- Purposes
- Adequacy
- Accuracy
- Retention
- Rights

- Security
- International transfers

This ensures that all data the company holds on its employees is held securely and is collected within reason – for example only having the data they need and only keeping it while they need it. This means their employee's data is safe and not invading their privacy.

Task 4

Is it ethical to use CCTV in a place of work?

For Arguments

- Makes people feel safer – CCTV can deter criminal activity as there will be evidence of the crimes being committed and they can be prosecuted
- Reduce workplace theft – having CCTV will deter employees from considering stealing company property as they would be caught through the recordings and could be prosecuted
- Reduce harassment – as everything is recorded on CCTV, anyone who harasses people can be caught and interventions can happen to prevent that harassment from occurring again.
- Creates a more productive workplace – as employees know they are being monitored; it makes it more likely for them to work to the correct level as they know they are being watched

Against Arguments

- It can go too far – having cameras watch the employee's every move can make them feel not trusted or like they are being spied on. This can hinder employee performance as they feel pressured the entire time
- Increase worker stress – constantly being monitored can add stress to the workers as, like I mentioned above, can make them feel pressured and worried if their boss doesn't think they are working hard enough
- False sense of security – CCTV only attempts to deter crime; it can't stop it. Security personnel are needed to stop crime.
- Cost – CCTV is often very expensive to setup and maintain and it will require dedicated personal to watch the CCTV

Is using the Freedom of Information act ethical?

For Arguments

- It can assist in people doing research into specific areas about public bodies
- Can hold public bodies accountable for wrongdoings as information is publicly available
- Helps maintain a level of transparency from bodies such as the government.
- Allows people to access statistics public bodies may try to hide – for example crime rates.

Against Arguments

- Can be an invasion of people's privacy – the FOIA can be used to request information about people who work in the public body, potentially breaching their privacy
- If a business works with a public body – the details of the business terms ad contract are publicly available, giving competing businesses the upper hand.
- Requires lots of hard work for the people who must respond and maintain the archive of information. This archive can include decades of data that must be backed up and

maintained to ensure they can respond to requests on demand. Requests can take hours to fulfil costing the company a lot of valuable time.

Task 5

What security measures do they have in-place?

Currently, the Oadby College has the following measures in-place:

- 3 access levels (student -> staff -> administrator)
- Staff must change their password monthly
- All IT rooms are locked when not in use
- All IT rooms must be opened via a swipe card that staff carry
- Equipment is secured to the tables
- CCTV covers the equipment and the hallways around it
- Software is installed to block certain websites
- Emails are scanned for viruses

How effective are the security measures?

The security measures are mostly effective, as they ensure that passwords are changed regularly in-case of a password being breached without the account owner knowing, everyone is given access to data on a need-to-know basis through access levels, meaning students can't access staff documents, etc. All equipment being secured down and with access control into the IT rooms helps prevent theft, and the IT rooms' CCTV is a further deterrent. However, the constant watching of CCTV could make the students and staff feel they are not trusted and could influence their work as they are always being watched. Emails being scanned for viruses also helps the network users not get infected with a virus which could in turn put the entire network at risk. Website blocking can also help filter out malicious sites and prevent people from accessing inappropriate sites.

Recommendations to improve security

To help increase security further, I would recommend the following security implementations:

- Cable Shielding
    - Cable shielding helps protect the data being sent down it from being intercepted, along with supporting the longevity of the cable and prevent interference during data transmission
    - This is done by protecting the data cables with dielectric insulation and metallic shields
- Visitor Logins
    - It is natural that sometimes staff won't be able to teach students due illnesses and similar. If they must use a computer, they should have a heavily restricted user access level and should have to sign-in and out of the IT rooms. This means they should only access the bare minimum of what they need to teach their students
    - They should also have a temporary ID badge and a swipe card that should expire at the end of the day if it isn't handed back in when they leave
- Anti-virus
    - All the machines should be installed with an anti-virus so that if students detonate malware on a machine, the anti-virus will block the attack before it can affect the network and the other computers inside of it
- Remote Monitoring (contains signing in/out)

  - Along with website blocking, they should also have a way of monitoring what is happening on the computer screens of students. This is to ensure they aren't attempting to breach any security and it also logs what times they use the machines and what they do on it, meaning if there was a network issues during a specific time the technicians could look and see who was using a computer at that time and what they were doing on it
- Encryption
  - Data send around the network should be encrypted to prevent the anyone from intercepting potentially confidential data
  - Data stored on network shares and on the servers should also be encrypted to prevent anyone from being able to access and read the data in the event of a breach
- Intruder Detection System
  - The networks sever should have intruder detection systems on them to detect and block any unauthorized access. For example, if someone who is not authorized to access the server breaks in, the IDS should detect that this has happened and block the connection from accessing the server. A log should be kept of these attacks and should be investigated to see what they exploited to access the server
- Disable the use of unauthorized peripherals
  - For example, a USB device, CD, etc.
  - This means no malicious devices can be inserted into the machines, this will help prevent breaches as these devices can often be used to run malicious scripts or contain files which can be used to hack a system on the network
  - This also prevents viruses from being exchanged between computers through the peripherals

Conclusion

To conclude, the college has implemented the basic methods of security and is maintain a decent security level. While there is still a lot to improve on, their current setup can help protect physical items being stolen, but their online data theft protection needs work. For example, they do not have encryption setup or any form of cable shielding to prevent any data being intercepted. They should also ensure that they can detect any breaches of security through Intruder Detection Systems so they can take the appropriate action to minimize data theft and leakage.