Scottish Social Services Council

Cyber resilience

Live scenario exercise

SSSC

Service A

Incident one

Monday 8am. You are the service manager.

Jess, one of the office administrators, asks if the gift card codes she sent you were what you were looking for. You have no idea what she is talking about.

- Jess says she received an email from you on Saturday morning.
- The email asked her to purchase £200 of gift cards for a raffle.
- The email said these were required immediately and she could claim the money back instantly on expenses.
- She bought gift vouchers on Amazon and responded to the email with the voucher codes.

Incident two

Tuesday 3pm

The eLearning provider used by the service sends out an email to say there has been a data breach involving their service.

- Usernames, email addresses, passwords and telephone numbers have been disclosed.
- The passwords were not hashed.
- The provider says that it takes security very seriously and has improved security following the breach. It recommends people change their password when they next login.

Incident three

Wednesday 9am

You learn that Andrew, a senior member of staff, has sent out thousands of emails to people inside and outside the organisation. Each email advertised pharmaceutical websites and an ‘anti-aging’ cure.

- Complaints are flooding into the service’s enquiries team.
- Andrew denies sending these emails.
- Andrew uses Office 365 email.
- Your IT provider says sensitive files Andrew had access to have been accessed and possibly copied.

Incident four

Thursday 10am

You are notified that the services website has been hacked. All links on the website redirect visitors to pornography. Nobody knows how to fix the website, but you need to do something quickly as it has been noticed by people who use the service.

- The member of staff who built the website no longer works here.
- The website uses the Wordpress CMS.
- The software has not been updated since the person left.
- Nobody knows where the website is hosted or who to contact.

Incident five

Friday 2pm

Over lunch all of computers in the service begin to stop working. They show a message stating that files have been encrypted and that you must pay a ransom to decrypt them.

- Files on the shared drive have also been encrypted.
- Work has ground to a halt.
- Attempts overnight by your IT provider to recover the files fails after the backups are discovered to be faulty.

SSSC

Service B

Incident one

Monday 2pm. You are the service manager.

You return from lunch to find the deputy manager is on the phone to BT. She looks worried. She tells you that someone has been trying to hack into the service's internet connection and BT are fixing it for her now.

- She was alerted to this by a call from BT.
- The caller asked to connect to her laptop to fix the issue.
- They are also connected to the desktop PC.

Incident two

Wednesday 5pm

You try to login to the service's email account but it asks you for a 2-step verification code. You haven't set this up and you don't recognise the last digits of the mobile number it says the code has been sent to.

- Other staff say they can't login either and nobody has setup 2-step verification on this account.
- You begin to receive phone calls from people who use the service. They are angry to have been sent emails demanding payment.
- Further calls come in from stakeholders warning that you are emailing malware out to people. You still have no access to your email account.

Incident three

Thursday 11am

The deputy manager tells you that she has lost her laptop. She left it on the luggage rack of the bus and it was taken by someone, either deliberately or by mistake.

- The laptop’s hard disk is not encrypted.
- There is a password on the user account. But will this keep the data safe?
- Returns for the Care Inspectorate were stored on this laptop and only older versions of the files are held on the USB backup.
- The service’s USB backup was attached to the device when it was stolen.

Incident four

Saturday 9am

Most of the staff have had their Facebook and Instagram accounts hacked overnight. Some even lost access to their email accounts.

- Only staff from this service seem to be affected.
- The affected staff are frequent users of the desktop PC in the office or have used it within the last month.
- The impact on staff has been devastating. Many have lost photos and messages stored on their social media accounts and keep no other copies of these.

Incident five

Sunday 2pm

You examining the services bank statements following notice from your landlord that they have not been paid rent for the month. The bank statement shows that they have been paid, although you do not recognise the account number.

- A member of staff recently updated the payee details following an email from the landlord.
- The email appears legitimate and shows no sign of being a phishing email. You forward it on the landlord.
- The landlord says the headers of the email show it was not sent by them, even though the sender and sender’s email look like it did.

Scottish Social Services Council

THANK YOU