Cyber attack!

Could you run services without IT for a week?

Lincolnshire COUNTY COUNCIL

Working for a better future

- On Tuesday 26 January 2016, Lincolnshire County Council was subject to a malicious software ('malware') attack on its IT system.
- The attack led to a shutdown of council IT systems as the authority investigated the malware’s impact.
- Eventually, council systems and online services were fully restored after being out of action for almost a week.

The Incident

- A member of staff opened a malicious attachment to email (zip file) at about 9.30am
- The incident was not reported until 12mid day
- Increased activity on network file stores was identified and the true severity of the incident was recognised
- The IT systems were shutdown to prevent damage whilst the precise nature of the threat and appropriate corrective action were identified

The Malware

- This was a “zero day” attack meaning this particular malware attack was not already known to the security industry
- A ransom demand was presented on screen ($500 bitcoins for each affected device)
- It encrypted files preventing access to the files it attacked

The Impact

- The email which introduced the malware spread to 300 users and over 47,300 files were encrypted by the time the shutdown was in place
- Damage was limited by containment action
- Staff were left with pens, paper and telephones
- Business continuity plans were activated
- The media were very interested

The Recovery

- 24 x 7 IT activity for the Council and its technology partners for 6 days
- Co-ordinated management of business priorities and IT activity at several levels
- Communication challenges
- Staff resilience and flexibility
- Catching up
- Valuable media support

Key Points

- A valuable exercise
- Time for people, time to reflect, time to tidy
- Review communication cascade regularly
- External validation of approach is valuable
- Wide range of stakeholders
- Information Governance
- Financial impact?
- Embrace the Press!

Things To Consider (1)

- Is Cyber Security on your corporate / strategic risk register?
- How good is your Information Governance awareness?
- Can your organisation communicate effectively without IT?
- What would your staff do for 5 days without IT?
- How would your service users be affected?
- Do your contracts include appropriate provisions?
- What would it cost?

Things To Consider (2)

- How would you close down your IT?
- Do your Services and your IT function understand each other?
- Are you BC plans based on an understanding of realistic IT recovery times?
- What are your BC plans designed to deal with and without?
- Do you know if they will work?

This was a relatively benign attack.

It could have been much worse!

Any questions?