Malicious Malware (Cyber) Attack
Lincolnshire County Council
January 2016

Lincolnshire COUNTY COUNCIL
Working for a better future

BACKGROUND & RISK

Lincolnshire COUNTY COUNCIL
Working for a better future

Background

- 2010; Five day IT ‘outage’ (hardware) exposed issues with LCC and key partner; timeliness, escalation, communication, and incident management (DR plan developed)
- 2015; Support service partner changes; contract performance (especially finance systems) become a distraction, and a reputational risk
- Neither of above dealt with as *business continuity* incidents
- Meanwhile … work to strengthen resilience and capacity (and ‘agility’) to respond to emergencies and disruptive events
- BC planning concentrates on ‘criticality’, ‘common supporting infrastructure’, ‘key partners/suppliers’, ‘incident management’ and ‘exercising’ (*especially identified business needs - social care*)

‘Reasonably foreseeable risks’

- ‘Cyber attack’ not currently on our ‘strategic risk register’ …
- But … foreseeable IT risks include failure of contract, loss of premises/server (*moving to data warehouse solution*), a prolonged loss of power (*beyond our back-up capacity*) … and … cyber attack!
- Key controls; ‘technical’ controls (*security systems*) & ‘user’ controls (*information governance*)
- New partner contractual obligations in place for response and disaster recovery … but not yet tested (*until now!*) due to distraction of overall performance, and the priority of fixing our financial system
- Work done on loss of premises (*following Oxford fire*)

THE INCIDENT

Lincolnshire COUNTY COUNCIL
Working for a better future

‘Council hit by £1m malware demand’ *(BBC News; 27th January)*

- User opens & shares an email-born ‘so-called’ ransomware
- User reports ‘unable to open’ shared file to colleague at 9.30am (*we believe the user see’s a ransom demand*)
- .zip file attachment seeks out files on shared drives and begins encrypting files
- 27 staff receive the email (*direct, or on shared network*)
- IT help desk eventually informed at 12.02pm (*no other reports*)
- Support team initially suspect the user’s device infected (*a daily occurrence – ‘low priority’*)
- Begin to identify (1.20pm) increasing activity on same network showing symptoms (*identify as a ‘high priority’)*
- ‘Ransomware’ contained demand for $500 in BitCoins (*per infected device*) for the decryption key
- (*Previously unseen, new variant of ‘JS Nemucod’ JavaScript Trojan downloader … AV signature did not recognise it, SIEM did not spot activity*)

Lincolnshire COUNTY COUNCIL
Working for a better future

‘Lincolnshire County Council “will not pay” cyber ransom’ *(BBC News 31st January)*

- 1.45pm SERCO Major Incident Team formed
- LCC Information Management Technology (IMT) informed at 3pm – BC Manager also informed
- Immediate authority ‘take all network shares off-line’ (network shutdown) until full extent of threat understood - users instructed via global email at 3.15pm
- 3.40pm liaison with AS to agree contingencies & update services with key IT systems
- 4.30pm Comms activity coordinated with CIO
- 5pm sample of virus shared with McAfee
- 6.50pm SERCO MIT *‘find a fix, or develop contingencies’*
- Containment (shutdown of all key systems) fully achieved by 7.30pm
- Providers working 24hrs for resolution
- Widely reported in media (*some inaccuracies*)
- Reported as a ‘crime in action’ to Police

Lincolnshire COUNTY COUNCIL
Working for a better future

‘Total IT shutdown over Zero Day attack’

(Computing.co.uk - 27th January)

- Shutdown lasted through Tuesday 26th to Saturday 30th Jan (3.5 working days)
- Affected some landline and mobile operability
- Limited IT service made available for social care (*safeguarding*) from Friday 29th
- 47,300 files encrypted (*network shares, largely used by teams within social care*)
- 300 devices affected – (accounts blocked) collected & quarantined
- Serco ‘Major Incident Team’; priority for LCC - find a fix, quick! Clean the system, gradual recovery, and return of assets

No data was stolen (some lost between last back-up and shutdown) - nor did we forward or share the virus to external contacts (*malware was not designed to do this*)

- No evidence this was a targeted attack
- We did not pay a ransom! Nor was it for £1million as widely reported

Lincolnshire COUNTY COUNCIL
Working for a better future

THE RESPONSE

Lincolnshire COUNTY COUNCIL
Working for a better future

‘Find a fix, quick! … manage the consequences’

- Incident Management Team (BC) established (27th) and set clear objectives for *managing the consequences* of the attack
- Worked in parallel with LCC’s Information Management Technology (IT) – *managing technical solution* with key partner (Serco)
- Overall policy direction – ‘Gold’ (Executive Director & Chief Information Officer)
  - Implement information gathering re impact and scale
  - Communicate with employees, members, public and media
  - Support continuation of services based on their level of criticality
  - Liaise with key partners and stakeholders
  - Manage all critical issues to their resolution

‘Criticality’

- Critical services ‘most’ vulnerable to loss of IT …
  - Adults and children’s services (*safeguarding and child protection data access*)
  - Specialist transport services (*electronic booking system*) for Lincs & Northants
  - Registration of death
  - Urgent payments (*including precept transfers to money markets*)
  - Customer Services Centre
  - Fire & Rescue Service
  - Civil emergency response (*County Emergency Centre*)
- Dynamic problem solving & ‘workarounds’
- Communication cascades, and challenges with no IT!
- HR and welfare issues (pay data fears, time off) – local discretion / interpretations
- Generic monitoring – all services invoked BC planning, or following policy

Battle Rhythm

- IMT first meets 2.30pm Wed 27th (agrees objectives)
- Membership as per most affected services and key individuals
- Paper trail (no IT)
- Meets twice daily until Tue 2nd Feb – with weekend sub-group teleconferences
- Closed at end of week when confirmation received ‘full IT services restored’
- SERCO and IMT incident management meetings continue throughout
- Key issues; communications / timings & sequence of meetings / competing demands and priorities

We will fully debrief and share all learning in near future …

EARLY LEARNING

Lincolnshire COUNTY COUNCIL
Working for a better future

‘Cyber attack triggers warnings to other councils’

IT learning; ***(CiSP & Gateway release from LCC)***

- Technical controls failed because it was a ‘new’ virus (*reliance on single supplier of AV – SIEM not effective*)
- User controls (*information governance*) failed; limited due diligence on behalf of user (*although from an apparently genuine source*)
- Some asset ownership information was inaccurate & out of date
- Replacing & cleansing 400 assets; conflicting priorities and a distraction of main effort v frustrated managers
- Reinforces the value of mandatory information governance training
- Using products which collate AV across numerous vendors may be better
- Ability to prevent users accessing network, quickly, is required
- Working with vendors produced a rapid response (*it’s in their interests!*)
- Swift procedure for escalation and close down is essential
- Luckily it was a relatively simplistic, ‘benign’ malware
- Resilience and welfare – 24hrs shift system to resolution

‘Lincolnshire Council forced to use pen & paper after ransomware attack’ *(IT Governance 2nd February)*

BC Learning …

- Some incident response systems failed – but we applied core command & control skills & agility in response
- Managed as a BC incident (*a ‘plus’ from previous experiences)*
- Dynamic BC planning / previously unidentified criticalities
- ‘Criticality’ is contextual (nothing to do with ‘importance’, or amount of additional planning required)!
- Contract ‘service response priorities’, ‘systems recovery’ priorities, and ‘recovery time objectives’ … are not the same thing
- BC contingencies need to cover different, and prolonged, timescales
- Ability to respond to civil emergencies intact (*alternative emergency centre*) operational capabilities maintained throughout *(see CCA duty)*

Lincolnshire COUNTY COUNCIL
Working for a better future

‘Council systems on the mend six days after ‘Bitcoin’ ransomware attack *(Lincolnite: 31st January)*

- Delays in initial response; but speedy containment, once scale of threat identified
- Timing! (*end of working day & impacts on financial processes*)
- Communications cascades (*no-one had an accurate list & we experienced failure of mobile mast in the middle of the incident!*)
- Interpretation and delivery of key decisions variable
- Displayed resilience, agility and flexibility?
- Users still logging in against instructions
- 23 asset ‘owners’ still not located (probable leavers)
- 56,000 emails in queue! Lot’s of back-record inputting, 2000 additional calls to CSC

- Service BCP needs more realistic aligning to technical abilities and recovery timescales
- What role – LRF, DCLG, cyber agenda?
- Keeping partners informed helped us
- There's nothing like the real thing!
- It really is wonderful not getting emails for a few days! ('*management by wandering', training, & lots of filing done!*)

We remained 'open for business' throughout, but …

- Another few days would have been crippling!
- In the circumstances … everyone did a great job

We've shared some of the 'headlines' … but, what do you think the dominant news story that week was?

Council order pensioner, 89, to cut back 'dangerous' yew hedge he has lovingly tended for 40 years” *(YouTube & Alan Titmarch!)*

It kept elected members very busy all week … it even led to Alan Titchmarch being asked to give his expert opinion ….

… it became the bigger story … and gave us some breathing space;

So I guess we should end by saying;

“Thank Yew for listening!”