Case Study: Managing a cyber attack

Summary

On April 5th 2016 at 11:14 am, Doncaster Council was hit by a cyber-attack. Malware – in this case a piece of ransomware called TeslaCrypt managed to get onto the council's network.
Doncaster's systems were well defended by the latest virus protection and in fact the site where the malware was hosted had been blocked through web browser filters. However, a member of staff needing the website – which related to social care functions – bypassed this by googling the website and going through the link provided in the search results. This let the malware attack in.

The attack was detected almost immediately because the ransomware displayed a pop-up page on the laptop demanding bitcoin payment to release the key that had been used to encrypt the files. This happened to a council laptop that was attached to the corporate network. The fast notification of the attack meant it was able to be quickly removed from the network and its wireless access was disabled.

Fortunately, Doncaster was able to contain the attack very quickly. A previously agreed recovery plan meant colleagues were able to rapidly put into action a staged recovery:

- The Assistant Director of Customers, Digital & ICT was informed immediately by a key ICT Manager and responded directly with the proposal of taking the Council network down to the Chief Executive, who agreed.
- A global communication was sent very quickly by the Assistant Director and then services were removed.
- Emergency Planning colleagues were contacted to set up an immediate Business Continuity emergency meeting.
- Business Continuity Plans across the council were initiated.
- The Communications team were asked to provide a consistent message for customers, partners, business areas and, if necessary, the media.
- The Cyber Security Incident Response Team (CSIRT) further investigated the issue and identified the virus and the extent of the damage to the council's assets. With this information

and in consultation with their external anti-virus supplier they were able to formulate a recovery plan.

- A phased recovery was completed by key ICT staff with all services restored by 11:30 pm. Defence products were brought back online first, with other services reinstated bit by bit, scanning for issues at each stage.
- The virus had encrypted three folders on the council's file stores. The council backs up information on a regular basis which meant that the files could be restored with no loss of data.

Their approach

Senior leadership

Key staff believe that had it not been for the senior leadership commitment to the issue of cyber security the incident would not have been handled so effectively and the impact could have been far worse.

The Chief Executive, Jo Miller, takes a keen interest in cyber security which raises the profile across the council. The Assistant Director of Customers, Digital & ICT and Senior Information Risk Owner (SIRO), Julie Grant, also performs a critical role and was willing to make far-reaching decisions on behalf of the organisation very quickly – in the face of an attack, seconds can count.

Having what they describe as an excellent SIRO makes a massive difference to the engagement with, and maturity of, cyber security at Doncaster; with cyber security recognised as a strategic risk for the organisation and key partners.

The SIRO is supported by the Technical Security and Compliance Office, Chris Whitechurch, and the compliance team which provides specific technical expertise in their relevant areas.

Across the business, Heads of Service are information asset owners who have responsibilities for their particular data assets, with the overreaching cyber security strategy coming from the Executive and SIRO. Regular reporting back to the executive via the SIRO ensures stakeholders, members and portfolio holders are kept informed.

An executive steer had meant the council had recently renewed its Cyber Incident Handling Plan and this was a key factor in the ability to respond so promptly. This strategy pushed a whole council approach, and also meant plans were fresh and up to date and all staff had a comprehensive understanding of their role in the event of an attack. Senior leadership were crucial to being able to set up that comprehensive framework for response and recovery.

Whole council approach The council has embedded a 'when not if' approach to cyber security, and have also made it clear that cyber security is a business enabler not just a side-line tech issue. It is seen as part of 'the fabric of the organisation', encompassing all staff. The approach taken in Doncaster has been to enable people to have confidence about doing the right thing. Staff, and even the public, are helped to help themselves when it comes to cyber security. Spam and phishing awareness e-learning is completed by all staff and councillors. Online safety features on the Doncaster Council website via http://www.doncaster.gov.uk/services/get-involved/online-safety. The Cyber Security Essentials badge is also displayed to increase confidence that Doncaster continually strives to keep all information safe and secure.

Technical response

The council has a number of technical controls in place to protect its assets including intelligent firewalls, anti-virus, vulnerability management, security incident and event management tools – but technical controls are only part of the cyber security equation. Ransomware uses techniques that are difficult for traditional anti-virus products to detect and it is only very recently that anti-virus vendors

have updated their products with a technical response to combat some of the challenges of ransomware. A key component of ransomware incident management is identifying the variant of the ransomware; this is key in understanding how to manage, stop, and sanitise the infection. A good working relationship with your anti-virus supplier can be a real bonus as they have a far deeper technical knowledge and intelligence that will help the recovery strategy.

A resilient infrastructure and back-up strategy in Doncaster meant that all affected files could be restored so no information was lost as a result of the attack.

Communications The council's Cyber Security Incident Response Plan recognises the importance of clear, consistent and concise communications during and after an incident. Information needs to be communicated at the right level to the right people at the right time.

It is important to recognise that the usual methods of communication, such as email or even telephone networks, may not be available during an incident and this must be planned for. During the incident in Doncaster, the quick global communication by the Assistant Director for ICT before services ceased followed by a quick emergency meeting including Emergency Planning and Communications triggered the Business Continuity Plans and the use of floor walkers within offices to answer questions and address any issues directly. Additionally, staff were posted on exits to ensure equipment was not removed from the premises and to answer any questions.

Communications after the incident are as important as during an incident. It is important for the business to understand what the incident was, what caused it, how the incident was handled, which lessons have been learned and what steps will be put in place to reduce the risk of it happening again. A brief was prepared for the Chief Executive and Directors to discuss the event and any lessons learnt.

Partnerships Doncaster is connected into the Yorkshire and Humberside Warning, Action and Reporting Point (WARP) which is an active community for technical staff in local authorities in the region to share concerns, advice and learning around cyber security. Doncaster were able to share their learning from this incident to the advantage of local peers. The incident was also reported into the national **Cyber Security Incident Reporting Portal (CISP)** which helps to collect and share technical information about different threats.

Key learning points

- Having malware and virus detection software in place meant the attack was identified quickly and the appropriate actions taken mitigating the impact of the attack.
- Keeping calm and swift decision making are essential. It is better to be brave and over-do than do nothing in these situations.
- Up to date anti-virus tools will not in themselves prevent attack, although they are extremely important in helping to mitigate the risk. It is a case of 'when' not 'if' an attack will occur, as new malware and means of attack develop rapidly, faster than the anti-virus capabilities can keep pace.
- All councils should have a plan for managing and recovering from a cyber incident.
- Senior leadership buy-in to the issue of cyber security is crucial to ensuring response plans are produced, kept up-to-date, and cover the whole organisation. Without this, the impact of the attack on Doncaster could have been far more damaging.
- The issue of cyber security is seen as embedded across the whole organisation in Doncaster and is the responsibility of all members of staff, not just IT colleagues. Staff feel empowered to report their concerns and act responsibly. This is a key means of mitigating attack, as most malware gets into systems through human action e.g. opening attachments, visiting risky websites, etc.

- All councils can benefit from joining their local WARP, and the national CISP, to receive and share information about cyber threats. Peer learning and the sharing of information helps raise the standards of all involved.