Cyber Centre of Excellence for Local Public Services

Fake cyber-attack tests business continuity plans

CASE STUDY

SOUTH STAFFORDSHIRE

South Staffordshire Council

The project

- Senior staff at South Staffordshire Council took part in a Business Continuity Day hosted by the CCoE.
- The workshop allowed staff to work through what might happen in an unexpected event, such as a cyber-attack, and whether their business continuity plans were adequate.
- A simulated six-stage ransomware attack allowed the organisation to examine the operational, technical, legal and strategic factors which would need to be considered in a real-life situation.

Why the CCoE?

- The CCoE is backed by the not-for-profit organisation iESE which has been helping transform and improve public services since 2004.
- Using its purchasing power, the CCoE can offer access to military-grade protection at high street prices.
- The CCoE continually evaluates new cyber protection products to take the guess work out of understanding vendors' claims – keeping users updated on the best and most cost-effective solutions available.
- The CCoE is supported by an Advisory Forum made up of some of the UK's leading experts in cyber security.

Results

- Council staff gained a better under-standing of the wide-ranging effects of a cyber-attack.
- The need for business continuity plans to be continually reviewed was highlighted.
- Overall, South Staffordshire found that as an organisation it was well prepared, which was a reassuring and positive finding.

Our mission is to ensure that the UK is the safest place to live, work and play in the digital world.

Around 25 senior staff from South Staffordshire Council had the opportunity to take part in a full day workshop hosted by the Cyber Centre of Excellence (CCoE) which was designed to check their business continuity plans through a staged ransomware attack simulation.

Mark Jenkinson, Assistant Director Community Services and the council's business continuity lead, said that as an organisation it was very aware of the risks involved with incidents that could affect delivery of services, including fire, flood and cyber-attacks. It also knew that one of the best ways to plan and prepare for such events was though having business continuity plans for each service, a strategy which served them well during the pandemic.

As an organisation it wanted to test these plans again using cyber as a real-life example. It first brought in a guest speaker in from Gloucester City Council which had experienced a cyber-attack to speak to staff about the impact of an attack on staff and residents. After this, South Staffordshire's service managers were encouraged to review their business continuity plans. "The leadership team always knew that we were going to do an exercise like the staged ransomware attack, but we wanted to make sure our staff were as prepared as possible," Andy Hoare, Assistant Director Business Transformation & Digital Technology at South Staffordshire Council explained, "The piece of work that we engaged Kurtis and the team to do was about testing those business continuity plans. It needed to be a real-life scenario, and a ransomware attack was the simplest one which people unfortunately hear about regularly. It was badged as a business continuity workshop because it was, but using cyber to enact those plans."

The workshop was designed to simulate a ransomware attack with six stages. Each stage was designed to focus on specific challenges, for example, operational, technical, legal and strategic. Key factors that needed to be considered during each stage included: budget limitations and priorities, time and resources, internal and public communication, governance, policies and practices.

At stage 1 attendees were told that the council had suffered a ransomware attack, all files had been encrypted and those responsible had demanded an amount of Bitcoin to restore the files. The hypothetical attackers gave 72 hours for payment before the files would be lost forever.

At stage 2 it was revealed the attack had also affected a local enterprise park – the consideration being whether the attack had spread from the council network to connected local third parties. At stage 3 the attendees were told to imagine that there was now mounting pressure from the press for updates on the situation.

At stage 4 the attendees were told to imagine that they had tried to restore a backup, but this had also been infected, while at stage 5 a back-up had been implemented but was out of date so there was still an issue of lost data.

Cyber Centre of Excellence for Local Public Services

CASE STUDY

"The piece of work that we engaged Kurtis and the team to do was about testing those business continuity plans. It needed to be a real-life scenario, and a ransomware attack was the simplest one which people unfortunately hear about regularly. It was badged as a business continuity workshop because it was, but using cyber to enact those plans."

Andy Hoare,
Assistant Director Business Transformation & Digital Technology at South Staffordshire Council.

At stage 6 the attendees were asked to consider the option of paying the ransom and what the potential effects of doing so could be. They were then asked to consider what the continued fall out would be and what would need to be investigated.

The attendees worked collaboratively throughout to assess the evolving situation, make critical decisions and then considered lessons learned and whether any adjustments were needed to the council's business continuity plans.

"Everyone engaged with the workshop day really well. It was designed to bring potential issues to the forefront so that if a real attack did happen, they would be more prepared. The good news was that South Staffordshire is prepared with business continuity plans and that was positive to see," said Kurtis Toy, Chief Executive of the CCoE.

Jenkinson said the day had brought about a lot of learning for everyone who had taken part and the organisation's business continuity plans would be refined as a result.

"The biggest learning was that as soon as a cyber-attack hits and you potentially lose access to systems you lose all access to your data. For example, planning applications follow a process and for a few days you can get by, but it is a statutory process with deadlines attached to it, and what the planning team realised was that they would need a list of live applications to work from. We have moved away from printing as an organisation, but we realised that having some things printed is crucial from a business continuity perspective," he added.

The council also learned that the communications sent out after a cyber attack should be co-ordinated, thought more about how teams who were unable to connect remotely would be able to work together in an age of hybrid working and also thought more about how personnel could be redeployed where necessary. "Each team started the day working on the problem in their own team. A bit before halfway through the day they started to realise they would be stronger and better working together. They started working out together what to prioritise and how to help each other," Hoare added.

In the feedback forms from the day, one participant said it was "an excellent workshop covering all aspects of a response to a major impact to council-provided services", while another said it had been an "excellent day and very thought provoking". Another attendee said the most impactful insight from the workshop was "the major impact cyber security can have on us and how real it is", while another said the day "raised awareness of the crosslinks with systems and other services and highlighted the reliance on digital services".

The majority of participants said the workshop had highlighted the need to continually review business continuity plans and to have some information printed and accessible. Many of those who attended said the day had been well facilitated, with one adding: "thanks for a really good session that highlighted just how real, likely and scary cyber-attacks are".

Hoare said he would recommend any organisation wanting to test their business continuity plans to carry out a simulated incident. "Is it scary – yes. Even if you think you are prepared you can realise that you are not as well prepared as you thought, which can make you feel uneasy. At the same time, if you have done no planning then think what that would feel like.

"Is it worth doing? I don't think you can ever be over-prepared for these things. I'd say to other local authorities to get your business continuity plans in place. We have put effort into this beforehand over a period of years and the business continuity plans paid real dividends, especially during the pandemic, but we still found some gaps. The benefit of doing an exercise like this is that you have to work the problem and when you work the problem you can see the gaps."

Do you want to discuss your current cyber defences? Drop us a line via

www.ccoe.org.uk
enquiries@ccoe.org.uk