Charity IT Leaders Quarterly Meeting
March 2020
Amba Hotel, Charing Cross

CHARITY IT LEADERS

Chair's Welcome

Dan introduced the meeting, and welcomed all attendees, including our sponsors, Databarracks, and representatives of United Christian Broadcasters who had come to introduce their broadcast work.

He then introduced the bit.ly being used to post questions and comments throughout the meeting. Dan explained that because of sensitive information being shared by some of the speakers Chatham House Rule applies to all conversations.

Dan also explained that confidentiality would be observed in the meeting notes, which would omit, by agreement with the speaker, to include a summary of one of the presentations.

United Christian Broadcasters

Richard Willoughby – Company Secretary. Based in Stoke-on-Trent

Opportunity to hear, watch or read the Word of God in a relevant and engaging way. Exist to see lives changed for good. £8.5m income.

Broadcast on national DAB radio. Available on 2 radio stations – UCB 1 and UCB 2. Also publishing – quarterly booklet – UCB Word for Today. Increasingly looking at digital editions. Also triggers a lot of donations, in addition to spreading the word of God. 95% of donations are voluntary.

UCB Prayerline. Offers prayer by phone, email and post. Trained Christian volunteers ready to pray for those who contact them.

www.ucb.co.uk

Ian De Soyza – infrastructure is mainly Microsoft. Cisco network. Custom built Lexus switches. Apps – more disparate. Raisers Edge on premise. HR and finance systems. Strategy is to start integrating back-office systems. Looking at cloud and Office 365. Large storage devices that mirror each other. 200 terrabyte.

First all-digital broadcaster in the UK. Christian organisation but not all the same variety of Christianity.

Databarracks, Bob Cawsey - Business Continuity and threats facing charities in 2020

Business continuity. Long-term supporter of CITL. Business continuity workshop, 16 April. [Click here to book]

You can't take someone else's business plan and make it work for your business. They all have to be bespoke and tailored to your organisation. However, there are common principals that you can apply across the board.

Business continuity also has to look at how to communicate to staff and suppliers.

They key thing is attitude. The plan is known and accepted at the top, but how do you embed the plan throughout the organisation?

March 2020. Already had several disruptive events:

Ciara and Dennis – storm impact. More storms on the way. Flooding has had a huge impact already this year. Streatham terror attack. Whole area was cordoned off. Impacts business. Another knife attack in Whitehall.

Microsoft Teams outage – went down in February because they hadn't applied their own SSL certificate into Teams.

Travelex – went down on NYE. Virus put into system 6 months previously. Enacted on NYE as optimal time to hit the system. Staff on holiday etc. Travelex out for a month and still suffering impact now. Didn't know if any data had been stolen from hacked systems. Reputational impact is still ongoing. Going to take a lot of work to repair.

Unexploded bomb found in Soho. Several streets were evacuated.

Brexit! Impact of that will be big potentially from supplier POV.
Coronavirus.
Lots and lots of BC events already in the year.

BCI best practices

Analysis – what are you trying to protect, why, how quickly do you need it up and running, what will the impact be.

Design – against the analysis. What do we do to mitigate.

Implementation – put those plans in place.

Validation – test it. Test it again. And again. Have to test multiple times to make sure it works and also to embed it within the organisation so it becomes second-nature.

Policy comes from the top of the organisation.

We all need to think about

People

Premises

Resources

Suppliers

Duty of care to staff. Need them to be able to continue business, but also have to keep them safe.

If the premises is offline where will they be? How do they work? How do you resource all this.

How do you interact with suppliers?

Workshop on 16 April:
Bird's Eye view of BC. IT infrastructure underpins everything.

People at the top have to cascade and embed. People on the ground have to know when to escalate.

BC is not just about IT DR. That might well underpin the recovery, but what else happens for the rest of the business?

Most plans follow a plan that looks as follows:

Develop plan, run business analysis, put plans in place, put facilities and resources in place. Then relax and forget. People leave for new roles. You get new products, people, suppliers. Plan becomes obsolete. Have an incident, and then start from scratch. Needs to be an ongoing process that is evolving and adapting with the business, staff changes and external factors.

Workshop – need to bring in/fill in the following info in preparation:

Risk assessment – Bob and James will review to tailor workshop to people's needs.

Questionnaire – 16 Qs to assess capability and readiness. Bob and James will let you know strengths and weaknesses, and direct where to focus. Share learning with group.

When looking at threats, consider mitigation. Do you:

Treat the threat

Tolerate the threat

Transfer the threat

Terminate the threat

Databarracks have a pandemic management guideline that they are happy to share with CITL. Has a trigger-point management plan.

Click here for links to the pandemic management documents.

Need to assess whether threats are short or long-term. Need to explore various scenarios. Eg not having access to the building but IT generally running. With pandemics you need to think about health & safety and transport etc. Need to consider the various scenarios and how long-term they= solutions might need to be.

Threats can be filtered into various scenarios and you manage the scenarios rather than every threat.

Laura – looking at immediate solutions, then month two etc. Crisis management v operating in a crisis. When does crisis management become BAU. Have to review particular crises as they are happening and keep adapting the plan accordingly. Also have to plan for recovery, eg getting the stuff back – apps, kit and equipment.

Planning for recovery has to be part of BC planning. What is the next step? How do we keep moving forward and integrate changing scenarios.

How do you persuade your FD or CEO to invest in the technology to mitigate these events which are likely to happen infrequently and ad hoc.

LSE, Laura Dawson – Running the meeting well

LSE is in the middle of continuity planning re Covid-19. Been in major incident and review planning meetings for five weeks, every two days.

Training day held two months ago. Used it in BC planning, but also in any meeting where you have to focus on making a decision.

Things to consider:

Who is the leader in the room. They MUST Chair.

In a crisis, it's NOT a democracy. In the NFP world, we will do all we can to avoid 'NO', and avoid conflict. BC planning is not the time for democracy. Someone HAS to take charge. It's not a chat. It's not a debate. We solicit opinion, but won't necessarily use it. 'Noted, not accepted' is a helpful phrase. Practice it, you may have to use it, a lot.

Be clear on the strategy.

MAKE A DECISION!!! Based on the information in front of you.

Comms and PR have to be last. They HAVE to hear everything else first. It has to reflect back out to the outside world.

Running a disaster meeting – The Scandi-method.

1. 2 minutes on situational overview summary
2. 1 minute for Chair to say what is the strategy and direction
3. 2 minutes – all present business units consider issues and ideas for action
4. 10 minutes – business units report for 1 minutes each on the issues and intentions
5. 3 minutes for Chair to give direction for business areas
6. 2 minutes for AOB and next meeting time

You have less than five minutes after a disaster to get a message out. Even if it's just;

'We are aware of an incident and are investigating. We will come back to you in 20 minutes'.

20 minutes later, 'We are still investigating. Our data is paramount. Our constituents are paramount. We will come back to you in 40 minutes.'

40 minutes later – next update etc.

It used to be days, now it's just minutes.

Inside world is desperately trying to fix things. Outside world is blogging, posting, instagramming, etc.

GDST, Dan Hall – Covid-19 planning

GDST have developed a 4 phase strategy to manage Covid-19

Kay priority – keep on teaching!!

GCSEs and A Levels – have to keep on teaching, can't postpone exams as too many other co-dependencies eg UCAS etc.

Phase 1 – individual staff need to work from home
Phase 2 – we need to reduce occupancy in our office
Phase 3 – essential staff only
Phase 4 – office shut

Splitting teams in half so some people in team are working remotely and others working as usual in the office. People will work a week at home then a week in the office. Deep clean at the weekend.

Teams encouraged to build plans around each of the scenarios so that once SMT decide to move from different phases the teams have a strategy in place to enact the next steps. Have identified various triggers and flash-points.

Have purchased additional laptop chargers and headsets for everyone. Handed these out at training about homeworking to make sure everyone attends the training.

Have to make decisions about which 'tools' to use eg Teams v Skype before people start working from home.

Weaknesses:

Some teams don't know how they will work – eg alternate weeks at home, rota, all homeoworking?

Impact on staff – health and wellbeing

Staff who don't have decent broadband – one Union has told members not to use home broadband for work purposes.

Security issues.

Collaboration.

What do we do with the post?? No-one at Trust Office to collect it or distribute it. Time sensitive items might be waiting for a response. Where will it be stored etc.

Policy is to avoid using home devices, and use the GDST-supplied devices. Haven't locked out home devices as this would be very difficult.

Use 80/20 rule. Can get 80% of people working. Focus on that, rather than the 20% who can't. Concentrate on the critical mass to keep the organisation going.

Bash through the changes – securely.

It's important to know when to consult, and when to tell. Peoples' input is important, but you can't accommodate everyone's ideas, and speedy, decisive action is needed in a crisis.

Support – how will you cope?

Give people a job. Others need to be flexible. Allocate tasks, roles and responsibilities beforehand.

Every school has a support plan for staff – in your role, this is how you get support. This is linked into Trust Office IT so they can step in and take over support in the event of school IT staff being ill or unable to work.

Managing payroll – can just re-run last month's BACS and sort out the differences later.

Scenario planning sessions

Various scenario planning exercises were carried out at each table. The following are the key takeaways:

1. Get the service desk to remember the trustees. Get them connected online, use collaborative tools etc.
2. Maintain best practice guidance.
3. Short survey online – have you worked from home. Run drills, get people to practice.
4. Flow charts.
5. Don't be driven by the edge cases – you have to work to the majority need.
6. Get a pulse going. Deliver info, tools etc in waves. Regular updates.
7. Focus on staff getting paid, but also suppliers.
8. Think about licensing.
9. Could you split your team?
10. Are there any consequences for projects eg products going out of licence.
11. Have you tested processes and procedures? Try and be ahead of the curve.
12. Being clear that you are not in 'business as usual' state. Helps to focus on the core parts of the business.
13. What can the organisation stop doing if the situation gets really bad.
14. Keep calm and carry on. Or panic and carry on depending on your POV!
15. Had O365. Had put MFA in place. People had the tools to work from home. Double global protect licenses.
16. Comms is crucial. Have a plan, be clear and timely. Send out regular updates for staff, and use multiple channels.
17. Have backup plans in place for eg payroll.
18. Make sure suppliers are prepped and are communicating their plans.
19. Reviewed Mind checklist for staff wellbeing.

20. This can be a positive in terms of trying new ways of working and new tech. This is the ultimate test and can improve working practices in future.
21. Staff wellbeing is paramount.
22. What is business essential, and how long for? This can change as the situation evolves.
23. What happens when portals can't manage demand eg O365.
24. What about the physical details eg the post, plugging in cables in the data centre?
25. Testing homeworking in small teams before you have to implement it as a whole organisation policy.
26. Utilise homeworking checklists.
27. QuickAssist.
28. Workstation assessment. Don't just sit there. Move around. Have a test plan. Do actual work, not just emails.