Business Resilience Checklist for IT Managers

Organisations will often make assumptions and have expectations about what IT departments will do in a business incident – without ever discussing it first with the IT department! This checklist is intended to help the IT manager control these expectations and assumptions during "business as usual", to avoid conflict and stress in the event of a business incident.

1) **Run a cyber breach incident scenario exercise with the senior management team:** Scenario exercises are a great opportunity to get the senior management team focussed on the big questions about business incidents, and a cyber breach is a key risk and a very plausible scenario to run. If you're in the room, you can answer questions and set expectations. For example, in a cyber breach scenario, explain that the cause of the breach needs to be found and isolated, the network may need to be isolated and infected IT services brought down then recovered *from the last uninfected backup*, which may mean that days or even weeks of business data is lost. What does the organisation say to its customers and other stakeholders? What work can be done without IT services? Do staff need to relocate and login from a clean environment to start recovery on an uninfected network? Use an exercise to start these conversations within the business at an executive level to get the buy-in you need to address any concerns in your ability to cope with a cyber breach.

2) Who owns each aspect of resilience and recovery? Be clear in the responsibilities: Organisations can expect IT departments to do absolutely everything in a business incident including finding a new building to house staff, instantly providing new and configured laptops, and re-routing the telephone system. Find out who owns business resilience and work with them to document a division of responsibilities, to make sure that nothing is missed or duplicated, and so this can be explained to the senior management team. In addition, some organisations expect their IT manager to also be the business continuity manager. If this is the case, be clear on this; get the authority from the senior management team and request their sponsorship to back up your decision making and to get you appropriately trained.

3) What are the priorities and what are the timeframes for IT recovery? End users are very impatient about IT downtime at the best of times. If all the IT services fail, your end users may well expect everything to be working again in minutes. This doesn't help the IT department, as there will likely be a limited number of staff working their way through recovering services. Recover using a prioritised list, with priorities and timeframes agreed with the business. This should also consider if partial IT recovery is acceptable - in terms of a single IT service's functionality being reduced, and also whether a set of critical IT services can be brought online while others are still recovering.

4) Map your IT service interdependencies: While the point above deals with business requirements for recovery, technical interdependencies will also need to be considered. There will be a whole list of IT infrastructure which wouldn't be known to the business but needs recovery before business services can be recovered. Also, you may need to carefully recover and synchronise application and database services to make sure that they send data to each other as expected following a recovery.

5) Balance user recovery and IT service recovery: Following on from the above, it's important that the organisation understands that the IT department may not only have to balance limited staff numbers between IT service recovery work, but also the work to get end users set up again. As with IT services, priorities and timeframes for recovery will help, but this time it's the priorities and timeframes of the departments that need to get working, again. This needs to be shared with IT in

advance of a business incident by the individual responsible for business resilience and recovery (agreed in number two above).

6) Write down the technical details of IT disaster recovery (ITDR): Techies can dislike writing things down and may see it as an insult to their ability, but it is important to document the technical detail of recovery in a "technical recovery plan" or "run-book". Even if an IT department member knows the IT service thoroughly, what if the IT incident happens when they are on holiday or after they leave the business?

7) Write down the management information for ITDR: The IT management team also needs a plan for use during a mass IT service failure. For starters, how is the decision made that IT services need to be halted and recovered from replicas or backups? How does the IT management team meet and make key decisions during such an incident? It's important that the IT management team has a tactical view of which services need to recover and in what order, and who is doing it. All this will help manage the incident, especially when it comes to complex decision-making. For example, it may be a creeping IT failure rather than something as sudden and obvious as a data centre fire.

8) Test it! ITDR tests can seem like a drain on time and resources, but the benefit comes in checking that it works and correcting any issues (in the technology setup and in the recovery plans), to reduce potential issues during a real ITDR situation. Many organisations test by setting up a closed DR sandbox network and recovering into this, to avoid any connection to the live environment and to avoid impacting live backups regularity.

9) Involve the organisation in ITDR tests: While IT departments may see this as additional difficulty in already complicated and time-consuming tests, it's good to involve end user departments so that they understand the ITDR process better and have a hand in it. Work with key business users to prepare test checklists before the tests, so that they can test the DR versions of recovered IT services in a controlled way. This will give IT another level of testing and will make departments a bit more prepared in the event of the real thing, and the checklists can also be used to validate IT recovery in a real incident.

10) Read IT service supplier contracts and press them for proof of their own resilience: Many IT departments are now responsible for far less in-house kit, with IT services increasingly hosted in the cloud, or in collocated data centres. Don't assume that cloud and colocation providers are doing everything right, or that they will provide you with a VIP experience if they have an incident which impacts your IT services. It's important to read the contract to understand what they are obliged to provide you, and that they can provide documented proof, such as a business continuity policy, and ITDR test reports.

About the author

David Davies is an award-winning business resilience and IT resilience consultant at Daisy Corporate Services. He has worked in IT resilience and recovery for more than 20 years, starting in a technical role at IBM looking after data backups and testing disaster recovery on very large enterprise systems. David then moved on to project management of disaster recovery testing, then into business continuity consultancy for the last 14 years. In that time, David has worked with more than 150 organisations as a resilience consultant, some medium-sized but the vast majority being enterprise-sized organisations.