Effective steps to cyber exercise creation

The following tips can help organisations create their own cyber incident response exercises.

This guidance is for organisations looking to create their own cyber incident response exercises. It's written for IT staff, cyber risk management, and business continuity teams in small to medium sized organisations. We've broken this guidance down into 9 manageable steps to ensure key elements are not overlooked.

If you're new to cyber exercising, or looking for off-the-shelf, generic exercises, please refer to the NCSC's free Exercise in a Box online tool, which contains materials for setting up, planning, delivery, and post-exercise activity.

Why conduct cyber incident exercises?

Organisations need to be able to detect and respond quickly and effectively to a cyber incident to reduce the financial, operational and reputational harm it can cause. Having effective cyber security and robust incident response plans and procedures in place is therefore crucial, as is the team's ability to follow them.

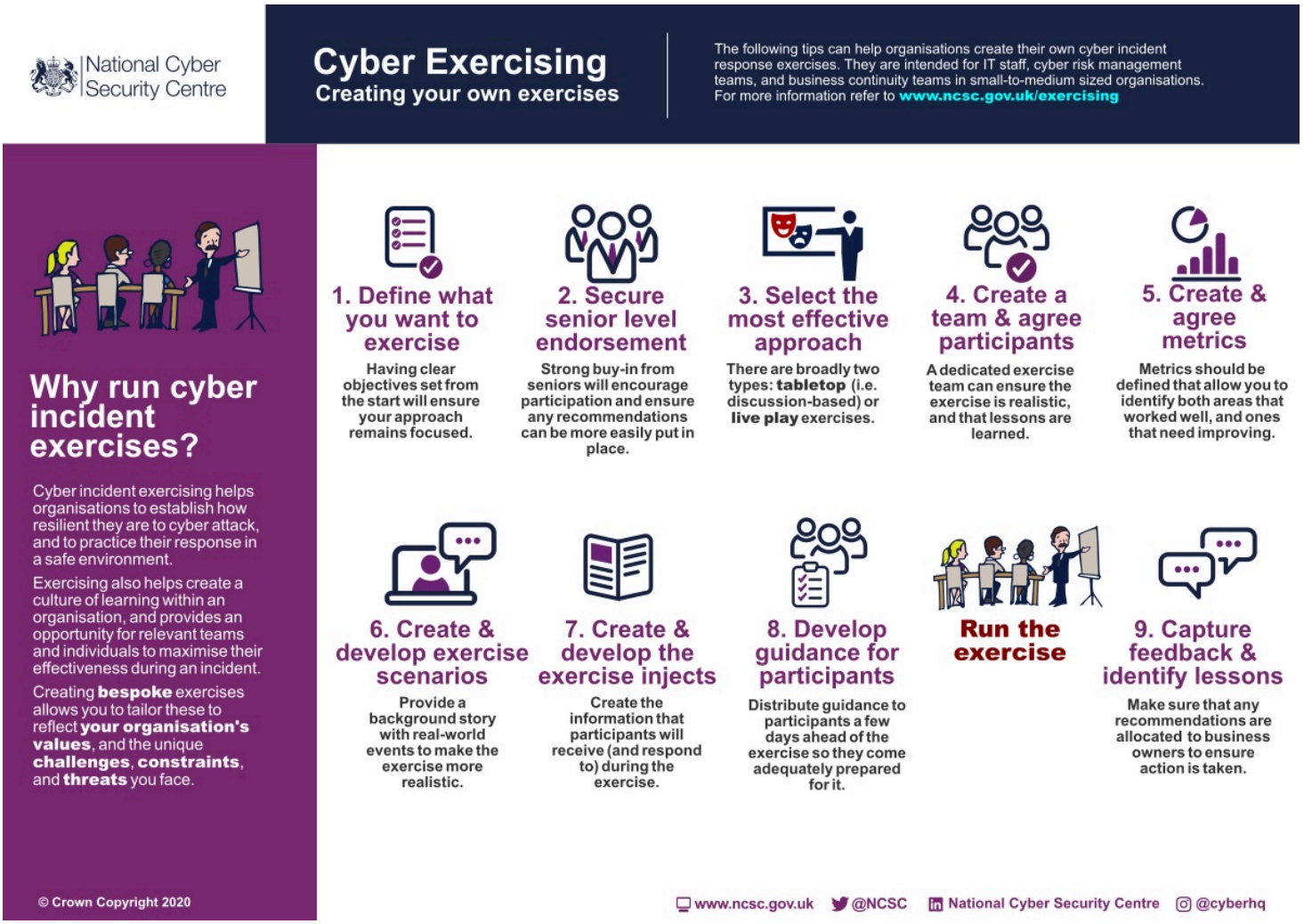
Cyber incident exercising helps organisations to establish how resilient they are to cyber attack, and practice their response in a safe environment. Exercising also helps create a culture of learning within an organisation, and provides an opportunity for relevant teams and individuals to maximise their effectiveness during an incident.

Creating **bespoke** exercises allows you to tailor these to reflect **your organisation's** values, and the unique challenges, constraints, and threats you face.

Note: You should **not** use exercising to create your response plans; these should

be in place already. If you don't yet have response plans, use workshops and consultations to help create them.

Infographic summary



A downloadable pdf is available at the foot of the page

Step 1: Be clear on what you want to exercise, and why

Having clear objectives set from the start will ensure your approach remains focused. Consider conducting a risk analysis to identify the most critical parts of the business, and use the exercising to test this first. It is also important to make sure the teams being exercised have clear plans that inform how they should

react to a cyber incident and that they understand. You will need well-defined response plans in place before you exercise; without these you have nothing to test. For more information on response plans, please refer to the NCSC's Small Business Guide: Response & Recovery.

Tips

- The cyber risks you decide to exercise should be based not only on the **potential harm** they can cause, but also on the **likelihood** of them materialising.
- Linking your exercise to your greatest cyber risks will significantly increase your chances of securing senior endorsement.
- Establishing a name for your exercise will help your colleagues differentiate it from any real-life events, therefore avoiding unnecessary confusion and creating a reference point for lessons flowing from it.

Step 2: Secure senior level endorsement

Management will want to know the rationale for conducting an exercise. Having strong buy-in from within your organisation will not only increase participation in an exercise, but also ensure any resulting recommendations can be more easily put in place.

Ensure those tasked with securing senior level endorsement have the skills necessary to communicate effectively at management level, and that they can clearly link the exercising activity to business and operational risks. They should explain:

- the areas exercising will focus on, and why
- the likely resources (human and financial) needed to deliver it
- the risks associated with **not** proceeding (and any alternatives)
- any related initial staff communication plans to maximise awareness and participation

- how you'll keep them updated on progress

Tips

Look to get approval for a programme of exercises rather than for individual ones. Not only is this more time efficient but it will also:

- demonstrate a coherent approach to your activity
- ensure key areas and/or issues can be exercised through focused individual exercises
- ensure lessons identified from one exercise are reflected in updated procedures ahead of the next

---

Step 3: Select the most effective approach/format

Exercising can be resource intensive, so carefully consider the type of exercise you want to run to best meet your objectives. There are broadly two types:

- **tabletop** exercises are discussion-based sessions where team members meet to discuss their roles and responses during a cyber incident
- **live play** exercises, where team members carry out their duties in a simulated cyber incident, usually in real time.

Alternatively, your objectives could better be met through a standard drill.

Factors to consider when deciding your approach will include:

- the objectives you have set
- the resources that are available to you
- the time available to both create and run the exercise
- the availability of key teams involved in your cyber incident response (for example, making sure all relevant teams are present can be challenging across multi-site organisations, or where remote working is the norm)

Tips

- Exercising should be used to strengthen and stress test your existing plans, not to create new ones. The latter is better achieved through other activities such as workshops and consultations
- Ensure your cyber response plans are as thorough as possible, and the right people in your organisation have access to them. Without this, you might get a confused and uncoordinated response by participants, which can damage morale

---

Step 4: Create an exercise development team and agree exercise participants

Creating a bespoke temporary team from across your business, no matter how small, will help you develop and deliver an exercise using a wider range of expertise. A dedicated team is better placed to:

- ensure an exercise is as realistic as possible
- help monitor activity during play
- identify any lessons resulting from the exercie

Make sure that you secure the right participation from across your business to allow you to meet your exercising objectives. This includes not just their job functions, but where necessary the appropriate level of seniority and any external stakeholders (such as contractors and third parties) that you might call upon during a cyber incident.

Tip

- Ensure that the timing of your exercise doesn't clash with any periods of key activity for your organisation, as this will affect participation in the exercise and your business's core operations.

Step 5: Create and agree exercise metrics

Define how you will measure performance during the exercise and what the expected actions of participants should be during each stage. Metrics should allow you to discover any areas of a response that worked well (and areas that require further development), resulting in the identification of clear lessons and recommendations. Make sure any agreed metrics are as comprehensive as possible and allow for the accurate and holistic interpretation of responses. Poorly focused or incomplete metrics will provide unreliable data, introduce bias and lead to false lessons. Metrics could include:

- adherence by participants to agreed response plans
- the time taken to conduct any key tasks
- the quality of decisions made and any response material produced (such as public messages)
- the effectiveness of any actions taken

Tip

- Consider using a feedback form with separate metrics to measure how well participants thought the exercise itself was developed and run.

Step 6: Create and develop the exercise scenario

Using your exercise objectives, start to create a scenario (or storyline) that your exercise will follow. Consider providing participants with related information to help make the exercise more engaging or realistic, such as a background story with references to real-world events in the news.

Tips

- Consider how you'd manage internal and external communications during an incident by building this into your scenario.
- Conduct some research to see if there have been any recent cyber attacks or threats against your sector, or on any systems you use. The NCSC's Weekly Threat Reports is a good place to start.

Step 7: Create and develop exercise injects

Create the information that participants will receive during the exercise (the 'injects'). These injects (which can be written or verbal) will provide information and updates for participants to assess. Use your wider development team to ensure these injects are realistic, and are sent to the right individuals in your business.

Tips

- Be clear what each inject is designed to do, and the expected actions it will prompt. Having unclear or unfocused injects may not only cause confusion, but may also prompt questions from participants which are outside of the remit of your exercise.
- Run any relevant injects past a technical expert to ensure what is being stated is credible and accurate (and more importantly, won't result in any consequences that could stop the remainder of your exercise).
- Ensure all exercise communications and material during play (including verbal), are started by using 'EXERCISE-EXERCISE-EXERCISE' followed by the exercise name. For example, if your exercise is called 'Powerplay', you'd start with the announcement 'EXERCISE, EXERCISE, EXERCISE. POWERPLAY'. This will ensure the exercise is not mistaken for normal business communications. This should be made clear in all participant exercise guidance documents.

Step 8: Develop guidance for the delivery team and participants

Create and distribute guidance to participants a few days ahead of the exercise so they are adequately prepared for it. This should include the exercise rules that define what is expected from them, and any contextual information you may want them to be aware of. For an example of how this might look, you can refer to the NCSC's free Exercise in a Box online tool. You should also make clear who else will be taking part (for example, by providing an exercise participant directory) and how feedback will be captured. Guidance for the delivery team itself could include:

- the exercise scenario and injects
- the exercise metrics
- any facilitator prompts
- a document to record feedback

Tips

- Even the best exercises will present questions from participants that you may not have identified during the creation phase. Provide players an option to put these questions to the delivery team during play, but also ensure any participant guidance states that they should not 'fight the scenario', even if they think it is not realistic.
- Ensure that participants realise that they will need to take decisions based on incomplete information (as this simulates the situation during the early stages of a real life incident).
- Ensure all participants and wider colleagues in your organisation are aware when the exercise starts and ends. This can be done through an email to all staff, supplemented with a tannoy announcement.

Step 9: Capture evidence and feedback, and identify lessons in a post exercise report

Record all key observations from participants, including on things that may not have worked so well. For an example of how this might look, you can refer to the NCSC's Exercise in a Box service. Give participants an opportunity to provide feedback, including on the exercise design and delivery. Any post exercise report should include:

- key observations/lessons identified
- associated recommendations
- allocation of recommendations to business owners to ensure action is taken
- a summary of participant feedback

Tips

- Consider conducting a short review session directly after the exercise ('a hot-wash') to capture the initial thoughts of key participants. This session can also be used to present your initial findings.
- Ensure any recommendations are implemented ahead of delivering subsequent cyber exercises.
- Capturing feedback on the exercise design and delivery should inform how future exercises can be improved.

PUBLISHED

3 February 2020

REVIEWED

7 February 2020

VERSION

1.0

WRITTEN FOR

Small & medium sized organisations

Public sector

/

Cyber security professionals