Cybersecurity Incident Response and Recovery Guide

The purpose of this short 'cybersecurity incident response and recovery guide' is to ensure that when a cybersecurity incident or data breach does occur, that the school already has a plan in place outlining how it will respond to the situation. Having a plan already in place will minimise the impact to the school. It will help the school recover and get back to 'normal' as quickly as possible.

- The cybersecurity incident response and recovery plan outlines the approach to improving the schools cybersecurity preparation in key areas.

- The authorised individuals/teams who are responsible for and coordinate the incident response and recovery plan need be listed in Table 1 of the school cybersecurity policy.

Short term priorities include:

- If an actual cybersecurity incident is suspected, the team leader of the cybersecurity incident response team (or their delegate) will call an urgent meeting (either in person or remotely) to assess the situation and to decide on next steps.

- If an actual cyber incident or data breach does seem to have happened, then the cybersecurity incident response and recovery plan should be activated. This gives the go-ahead for a series of already-planned and approved specific actions to take place. These actions are designed to protect the school systems and data, and to minimise the impact of a suspected cyber-incident on the school and school community.

- The most urgent immediate priority is to ensure that the school policy on 'Data Backup and Recovery Policy' is in place and up to date. This is to ensure that the data backup process is working to protect schools data from being deleted, damaged or corrupted by a possible cyberattack. Refer to the 'Data Backup and Recovery Policy' section of the 'School Cybersecurity Policy' for relevant details.

Other immediate /short term priorities include:

- Turning off/disabling the school network, school computers, WiFi and Broadband from the 'outside world', so that all school digital and online systems are no longer available or accessible. This disables user access to all online school systems.

- Contacting the school IT technical support company to seek their technical support to review the situation, determine the impact on the school systems and data, identify the source of the cyber-incident, and assist in planning a phased recovery.

- Determining if a data breach took place and if so, if the incident needs to be reported to the Data Protection Commission (DPC), https://forms.dataprotection.ie/breach-notification

Longer term considerations include:

Planning how the school would respond to a future cyberattack or data breach is also a critical aspect of a school cybersecurity plan.

- The first step in putting in place a cybersecurity incident response and recovery plan is for the school cybersecurity team to have a meeting to discuss what's involved.

- As part of this process the school cybersecurity leadership team needs to review the following relevant documents which are located in the 'Leadership' section of https://www.oidetechnologyineducation.ie/technology-infrastructure/data-security/ .

  Relevant documents:
  1. Assessing School Cybersecurity Readiness
  2. Cybersecurity Training For School Leadership (Powerpoint Presentation)
  3. Cybersecurity Incident Response and Recovery Guide (ie this guide)
  4. **School Cybersecurity Policy Template – Key Document**
  5. Cybersecurity - Roles and Responsibilities Table

- Following a review of these documents the school cybersecurity team should be in a better position to see how the cybersecurity incident response and recovery plan fits into the overall 'School Cybersecurity Policy' based on the 'School Cybersecurity Policy Template' document provided.

Run a Cyber-Incident Simulation Exercise:

- This process can assist schools in establishing how resilient they are to cyberattack, and to explore their response in a safe environment. It 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.

- Part of the incident response and recovery planning process is to have already carried out a 'cyber-incident simulation exercise' which could be pre-tested during the first term of each school year.

- The purpose of this 'cyber-incident simulation exercise' is to improve how a school can prepare in advance for an actual cybersecurity attack or data breach, and to minimise any issues or 'panic' that might otherwise occur, during an actual cyber-incident.

If the School Cybersecurity team have any related questions on this area they can email Oide Technology in Education at ictadvice@oide.ie