Stronger Charities.
Stronger Communities.

The Wheel Cyber Incident Response Plan

Due to the technological focus of responding to cyber threats, a specific plan is in place for cybersecurity incidents.

1. Declare a crisis

2. Assemble the Business Continuity Team

3. In case of cyber incident, this team will include the Information Systems Manager

4. Other staff who by the nature of their roles may be well placed to support the Business Continuity Team, may be drafted temporarily into the team,

5. The Business Continuity Team will assess the crisis and understand the risks to the organisation, with reference to the Risk Register

6. The Business Continuity Team will confirm the nature, severity (e.g., minor, significant, critical) and scope (affected systems, data, or users) of the incident (e.g., malware, phishing, ransomware).

7. All line managers will check in directly with their team members by any appropriate means to ensure they are aware of the breach and to check on their wellbeing, bearing in mind that sensitive staff details could be released.

8. The preferred channel of communication with staff will be through Microsoft Teams

If the cyber incident has affected access to Microsoft Teams, emails or instant messaging, other means such as phone calls, WhatsApp, video calls may also act as a communications channel for staff.

1. A briefing, created by the Communications Team will be circulated to the Board of Trustees and staff with instructions on how to deal with queries and information requests.

2. The Communications Team will formulate messages to be delivered to key stakeholders and the media and monitor for response.

3. Report any data breach to the Data Protection Commissioner (DPC) within the statutory timeframe

4. Engage with our IT providers to contain the threat and prevent the incident from spreading and mitigate vulnerabilities as much as possible. These steps will include

a. Restrict access to sensitive systems or data until the threat is neutralised.

b. Contain the Threat by isolating affected laptops (e.g., disconnect from the network) to prevent the incident from spreading.

c. Restrict access to sensitive systems or data until the threat is neutralized.

d. Eliminate the malware, ransomware, or other malicious software using antivirus tools or manual intervention

e. Address Root Cause by identifying and fixing the vulnerabilities that allowed the incident (e.g., unpatched systems, weak passwords, phishing attacks).

f. Conduct a thorough review to ensure all traces of the threat have been removed.

1. Once the organisation has confirmed the threat has been removed or contained, the team will begin the steps of recovery.

a. Reconnect isolated systems once they've been confirmed clean and secure.

b. Restore data from backups if any information was lost or corrupted.

c. Verify that all systems are functioning normally, and no additional vulnerabilities remain.

d. Continuously monitor to ensure the attacker does not return or exploit other weaknesses.

1. As the crisis is becoming resolved, the Team will begin a phase of assessment and improvement to prevent future incidents and/or improve our response.

a. Record details about the incident, including how it was discovered, the type of attack, and affected systems or data.

b. Document all actions taken during containment, eradication, and recovery including any associated expenditure (Appendix E)

c. Assess the efficiency of our response to identify strengths and areas for improvement.

d. Conduct a Post-Incident Review - analyse how the incident occurred and determine what could have been done to prevent or detect it sooner.

e. Refine our incident response plan, security protocols, and employee training to strengthen defences.