Why understand your cyber risks?

The risks and impact of a cyber attack upon your educational setting is something of which you are likely already aware. The consequences of a successful breach can, however, be much more severe for the people whose information you have a responsibility to protect.

To operate effectively, educational establishments collect and retain a significant (and often sensitive) range of data. If this information was to fall into the wrong hands, the impact would result in significant inconvenience and potentially put individuals at risk of fraud or other crimes.

How do we safeguard the information we store?

A successful attack will impact upon your reputation as a custodian for this type of information. The people whose data you handle and store will have expectations about how you protect their data and will expect you to plan to manage the risks accordingly and proportionately.

Working with Cyber Culture will give you the opportunity to consider what measures you have in place and test whether they are adequate.

Cyber security risk management and mitigation is no different to the other risks that a senior leadership team must manage.

Cyber Culture can help you assure the measures you have in place.

Educational settings all gather and store personally identifiable and sensitive information, including:

- Medical information
- Financial records
- Child safeguarding information

How can we improve our cyber readiness?

As always, there is a balance to be struck between the costs of being prepared and the costs of recovery from an incident.

Organisations who find themselves victims of a cyber attack find the recovery costs to be multiples more than the associated upfront protective measures.

Ensuring your staff understand the contribution they can make is one of the most cost-effective ways of improving your overall preparedness.

Next steps

Working with Cyber Culture will significantly improve the overall understanding of cyber risks across your leadership team - and the training you receive will be engaging and interactive.

You will get the opportunity to practice responding to a typical incident and be able to assess your team's capability. Role-playing a successful and well-considered response is an excellent way to evidence your preparedness and showcase knowledge and understanding.

Cyber Culture has several packages you can commission for leadership briefings and/or briefings for wider staff teams, enabling you to:

- Recognise risks and how to reduce them

- Understand the measures required to protect your systems and data

- Embed the skills, knowledge, and experience required to respond

- Engage more effectively with your IT systems providers and confidently understand how they protect your organisation

Act now to book your tailored session

Email **contact@cyber-culture.org** or call us on **07484 161791** to start a conversation about how Cyber Culture can help you