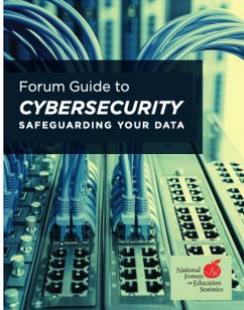


Publication Summary

Forum Guide to Cybersecurity: Safeguarding Your Data



Security is an increasingly critical consideration in education agency operations, including the collection, management, and use of education data. Education agencies are data-rich environments, which makes state education agencies (SEAs), local education agencies (LEAs), and schools prime targets for cybersecurity threats. The number, scale, and severity of cybersecurity incidents in education agencies have increased in recent years. Major incidents, such as ransomware attacks and denial of service attacks, have hindered routine operations and, in some cases, shut down schools for weeks at a time. These types of incidents are expected to increase in the coming years, making cybersecurity an important topic for education agencies.

The National Forum on Education Statistics (Forum) developed the *Forum Guide to Cybersecurity: Safeguarding Your Data* to help states and districts proactively prepare for, appropriately mitigate, and responsibly recover from a cybersecurity incident. It provides recommendations to help protect agency systems and data before, during, and after a cybersecurity incident and features case studies from state and local education agencies. It aims to provide information that will be helpful to a non-technical audience of education stakeholders, including SEAs, LEAs, parents, and board members, who are concerned about ensuring the security of systems, information, and data in education agencies.

The resource includes a glossary and the following chapters and appendices:

- **Chapter 1: Cybersecurity in State and Local Education Agencies** defines cybersecurity and illustrates the extent of cybersecurity incidents, threats, and vulnerabilities.
- **Chapter 2: Before a Cybersecurity Incident—Planning and Prevention** discusses planning activities and proactive measures that agencies can take before a cybersecurity incident to prevent an incident in the future.
- **Chapter 3: During a Cybersecurity Incident—Mitigation** reviews measures that agencies can take when a cybersecurity incident has occurred to minimize the impact of the incident.
- **Chapter 4: After a Cybersecurity Incident—Recovery and Restoration** describes response activities after a cybersecurity incident has occurred to restore systems and their data.
- **Chapter 5: Case Studies from States and Districts** presents case studies from SEAs and LEAs that have planned for or experienced a cybersecurity incident.
- **Appendix A: Cybersecurity Checklist** contains a checklist of tasks and activities to be undertaken before, during, and after a cybersecurity incident.
- **Appendix B: Resources on Cybersecurity in Education Agencies** provides a sample list of federal and state resources on cybersecurity.

The *Forum Guide to Cybersecurity: Safeguarding Your Data* is a product of the National Forum on Education Statistics and is available on the Forum website at https://nces.ed.gov/forum/pub_2020137.asp. The information and opinions published in the guide are the product of the Forum and do not necessarily represent the policies or views of the U.S. Department of Education, the Institute of Education Sciences, or the National Center for Education Statistics.