Forum Guide to Cybersecurity: Safeguarding Your Data

National Forum on Education Statistics

National Forum on Education Statistics

Mission: To plan, recommend, and develop education data resources that support local, state, and national efforts to improve pre-kindergarten through secondary education throughout the United States.

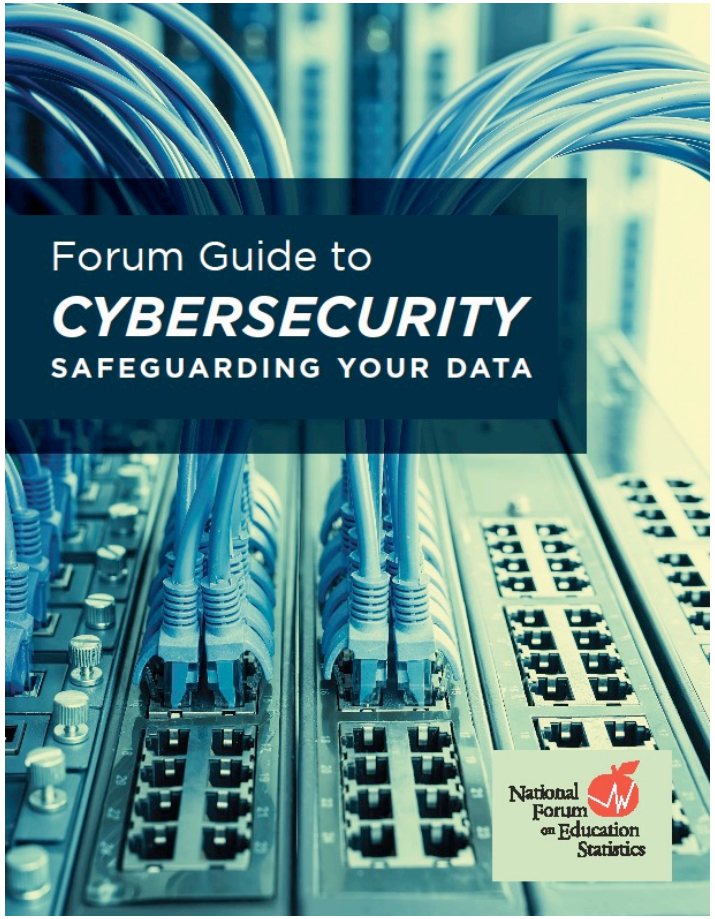
Members:

- Representatives of offices of the U.S. Department of Education and other federal agencies
- Representatives of state and local education agencies (SEAs and LEAs)
- Associate members from U.S. territories, Regional Educational Laboratories (RELs), and national education associations

Forum Guide to Cybersecurity: Safeguarding Your Data

Purpose

- To help education agencies proactively prepare for, appropriately mitigate, and responsibly recover from a cybersecurity incident.
- To provide recommendations to help protect agency systems and data before, during, and after a cybersecurity incident.

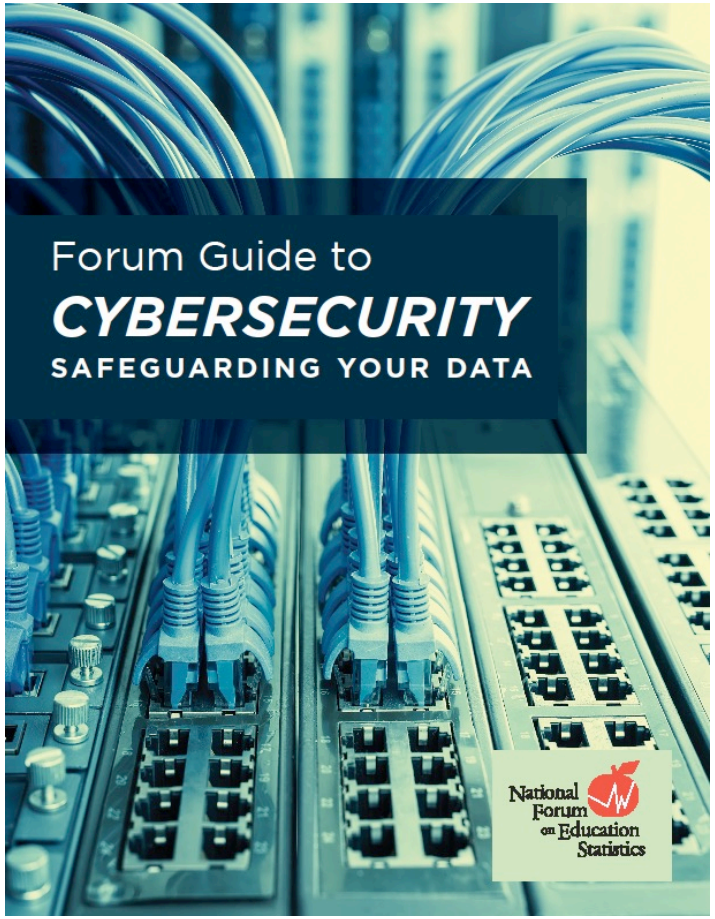


Forum Guide to Cybersecurity: Safeguarding Your Data

Audience

Education stakeholders who are concerned about ensuring the security of systems, information, and data in education agencies, including:

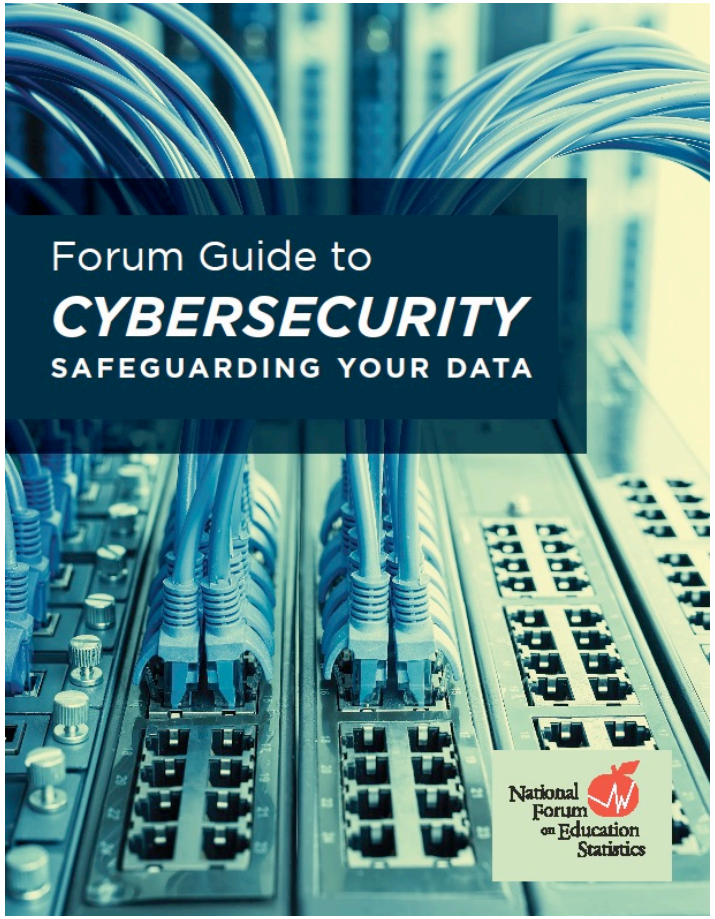
- SEAs
- LEAs
- Parents
- Board members



Forum Guide to Cybersecurity: Safeguarding Your Data

Chapters

1. Cybersecurity in State and Local Education Agencies
2. Before a Cybersecurity Incident: Planning and Prevention
3. During a Cybersecurity Incident: Mitigation
4. After a Cybersecurity Incident: Recovery and Restoration
5. Case Studies from States and Districts



What is Cybersecurity?

Cybersecurity is the protection of technology systems and networks—including all devices and tools connected to them—against intentional or unintentional threats, vulnerabilities, attacks, and exposure.

Any network-connected technology system or device can be vulnerable to a cybersecurity incident, including, but not limited to:

- Information technology (IT) and data systems
- Security systems
- Student information systems (SISs)
- Communication systems
- Desktop and laptop computers, tablets, smartphones, and other computing devices
- Facility operations systems and field monitoring devices
- Printers and peripheral devices
- Smart classroom and smart building devices

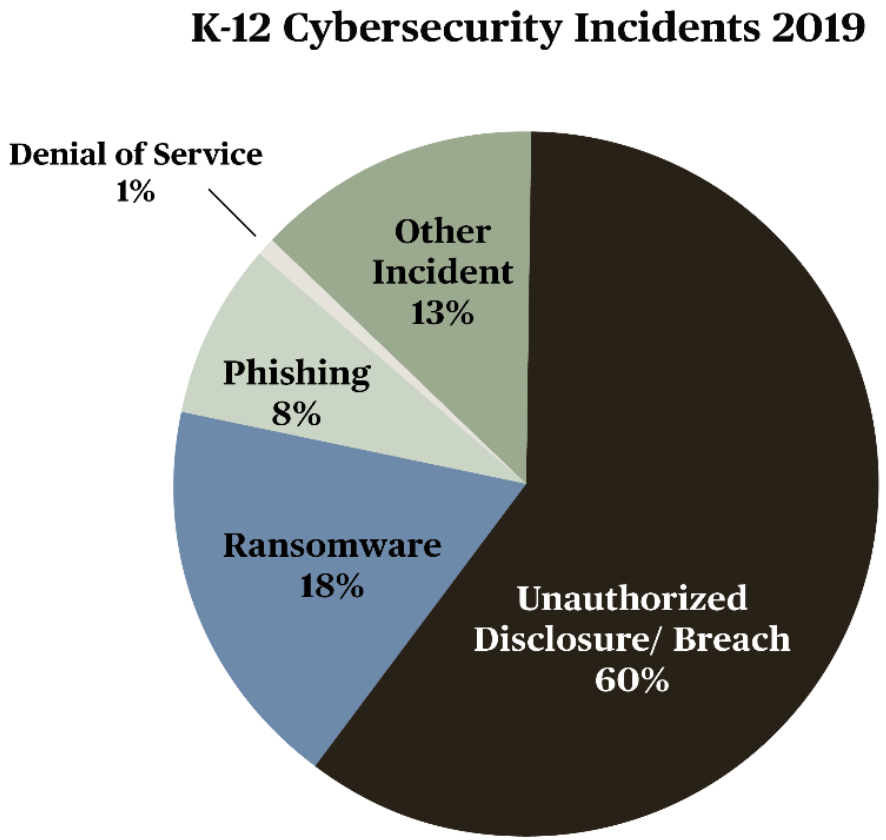
The Impact of Cybersecurity Incidents

Education agencies face a wide variety of cybersecurity threats and vulnerabilities. Cybersecurity incidents can

- significantly disrupt education agency operations;
- compromise the privacy, safety, and integrity of important agency assets; and
- engender fear and mistrust amongst an educational community.

Cybersecurity Incidents in Education Agencies

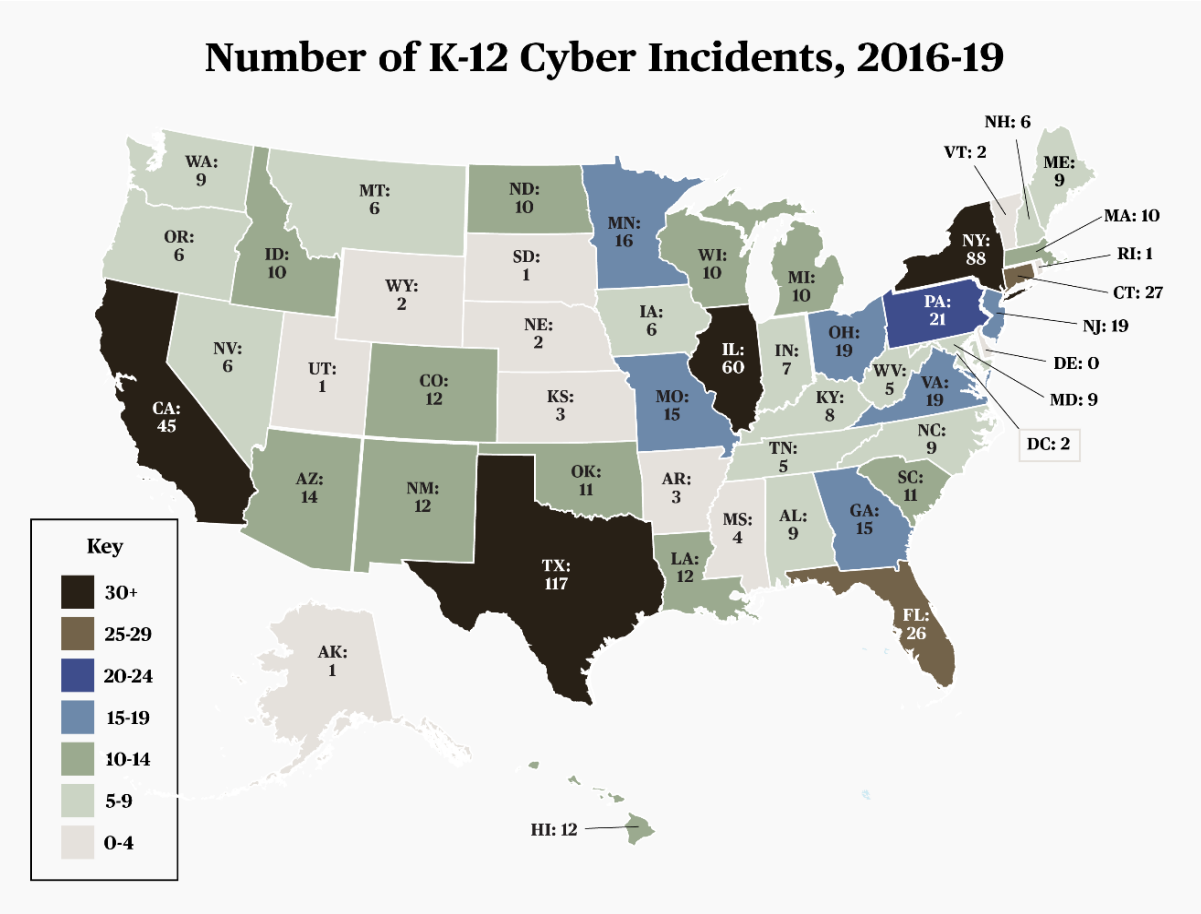
- As technological innovation has advanced, cybersecurity incidents in education agencies have also increased.
- Nearly three times as many incidents in K-12 agencies were reported in 2019 than in 2018.
- Schools and colleges were the second-highest targets of ransomware in 2019.



SOURCE: Levin, D. A., "K-12 Cyber Incidents," 2019.

Cybersecurity Incidents in Education Agencies

Nearly every state in the nation has been affected by at least one publicly-disclosed cybersecurity-related incident in a public K-12 education agency between 2016 and 2019.



SOURCE: Levin, D. A., "K-12 Cyber Incident Map," 2016-19.

Potential Consequences of Cybersecurity Incidents in Education Agencies

Incident Type	Potential Consequences
Phishing messages	• Identity theft • Password disclosure • Provide access credentials for secure data systems • Unauthorized data disclosure
Unsecured network and Internet connections	• Identity theft • Malware infections • Password/credential theft • Unauthorized disclosures and access to connected systems
Payroll system vulnerabilities or attacks	• Financial theft or fraud • Identity theft • Theft of financial information (for example, bank account numbers)
Hacked notification/ automated call system	• Inciting panic by sending false messages of emergencies • Theft of personal contact information • Threatening message sent to parents or students

Key Recommendations Before an Incident

- Identify the risk landscape by developing a comprehensive inventory of all agency assets.
- Implement high-impact, low-cost solutions to better protect education agencies.
- Provide training for all staff, students, and end-users of information and data systems.
- Secure agency networks through monitoring, scanning, and segmentation.
- Assess existing systems and address potential system vulnerabilities.
- Monitor and automate security to identify potential threats and protect against incidents
- Establish a cybersecurity response plan that identifies all actions that need to take place to protect agency systems and data before, during, and after a cybersecurity incident.
- Review policies and procedures to ensure cybersecurity and related issues (such as data security, privacy, and data retention) are addressed.
- Create and implement coherent policies for account security and identity management.

Key Recommendations During an Incident

- Confirm the incident by examining the available evidence and information.
- Determine the scope, severity, and impact of the incident.
- Initiate a response in accordance with the cybersecurity response plan.
- Prioritize essential business functions to focus response efforts.
- Take offline or shut down any affected systems, hardware, devices, or software if the threat remains active and has not been mitigated.
- Initiate communication with legal personnel and agency staff.
- Initiate communication with external stakeholders when appropriate, including the agency's cybersecurity insurance provider, law enforcement, parents, and other parties.

Key Recommendations After an Incident

- Investigate the incident to determine the root cause of the incident and implement strategies that will minimize the chance of future recurrence.
- Replace, upgrade, restore, and/or retire any systems, hardware, devices, and/or software that were affected by the incident.
- When recovering from a major incident, consider temporarily reassigning staff, hiring new staff, or contracting with external groups to assist with recovery tasks.
- Retrieve any data that were lost due to the incident or were collected when systems were offline.
- Evaluate the response plan and use the results to improve cybersecurity measures.

The Bottom Line

Education agencies need to be proactive in protecting their systems and data from threats, strengthening weaknesses and vulnerabilities, and planning for potential future incidents.

Case Studies from States and Districts

The resource includes case studies that detail the actual experiences of SEAs and LEAs planning for and responding to cybersecurity attacks, threats, and vulnerabilities:

- Developing a data breach response protocol
- Implementing a cybersecurity program
- Responding to an SQL injection attack
- Responding to a vendor data breach
- Recovering from a ransomware attack

Appendices

- **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.

Cybersecurity Working Group

Jay Pennington, Chair, Iowa Department of Education

Kristen DeSalvatore, New York State Education Department

Michael Gerszewski, Bismarck Public School District (ND)

Stephen Gervais, San Bernardino City Unified School District (CA)

Phil Grace, formerly of Heber Springs School District (AR)

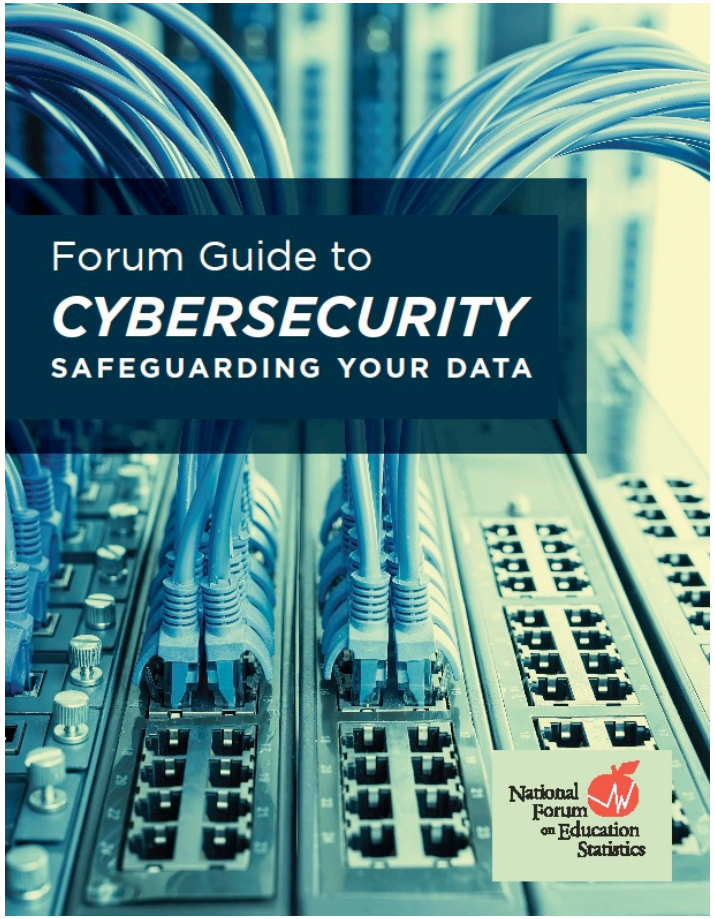
Georgia Hughes-Webb, West Virginia Department of Education

Rachel Johnson, Loudoun County Public Schools (VA)

Allen Miedema, Northshore School District (WA)

Steve Smith, Cambridge Public Schools (MA)

Andrew Swickheimer, Noblesville Schools (IN)



Forum Resources

Forum Guide to Cybersecurity: Safeguarding Your Data
https://nces.ed.gov/forum/pub_2020137.asp

For more information about the Forum, please visit
https://nces.ed.gov/forum/index.asp

Download free Forum resources at
http://nces.ed.gov/forum/publications.asp

The information and opinions published are those of the Forum and do not necessarily represent the policy or views of NCES, the Institute of Education Sciences, or the U.S. Department of Education.