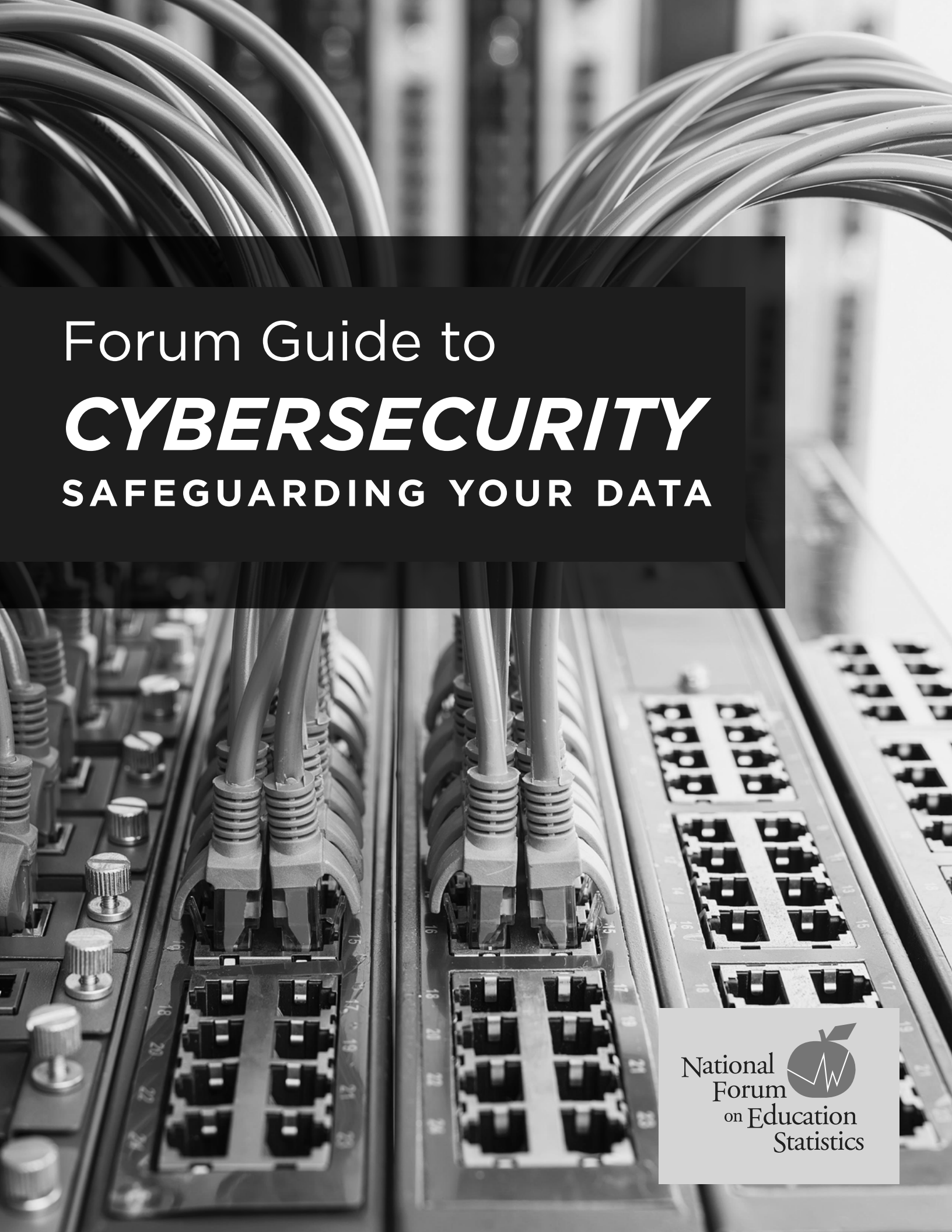
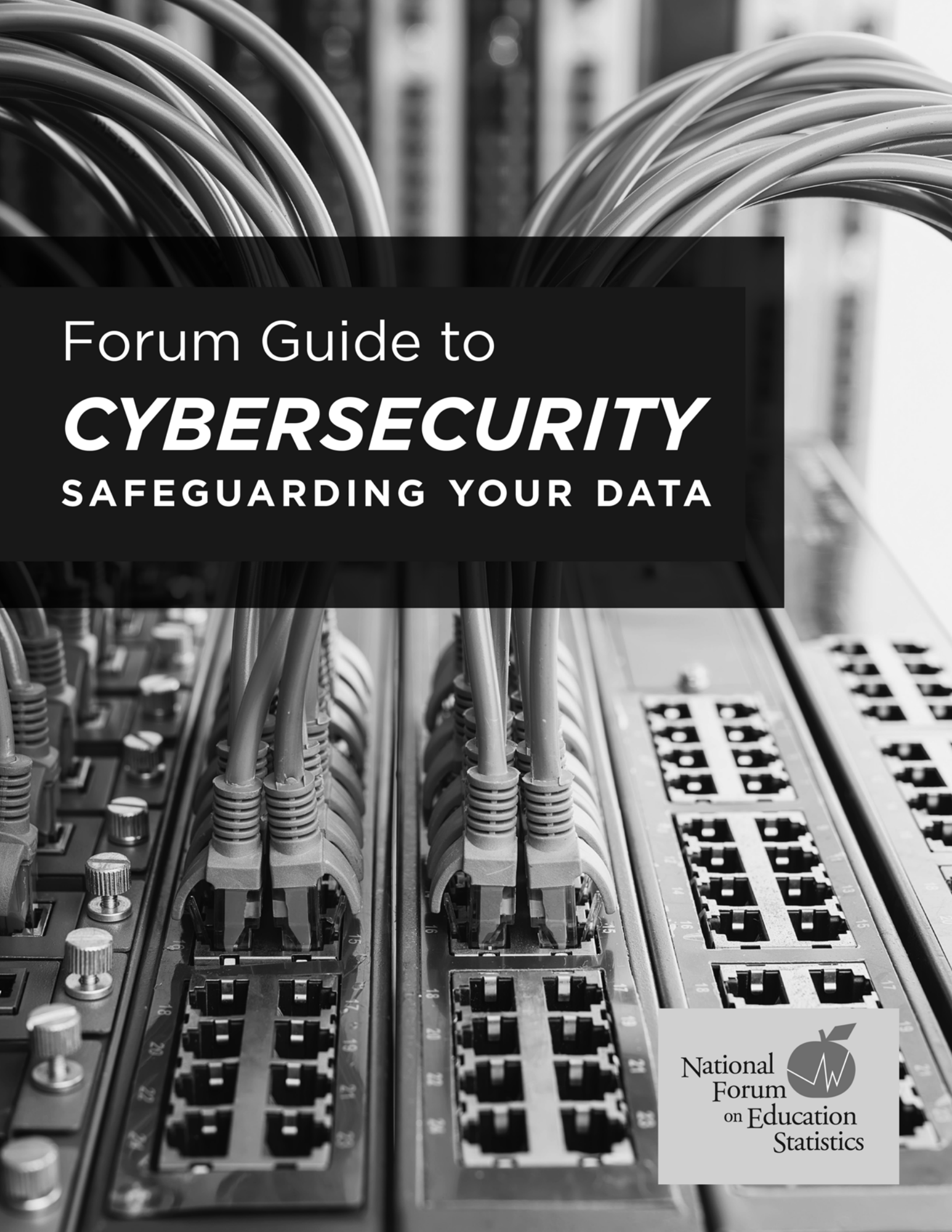


Forum Guide to
CYBERSECURITY
SAFEGUARDING YOUR DATA

National Forum on Education Statistics



Forum Guide to
CYBERSECURITY
SAFEGUARDING YOUR DATA

National Forum on Education Statistics

National Cooperative Education Statistics System

The National Center for Education Statistics (NCES) established the National Cooperative Education Statistics System (Cooperative System) to assist in producing and maintaining comparable and uniform information and data on early childhood, elementary, and secondary education. These data are intended to be useful for policymaking at the federal, state, and local levels.

The National Forum on Education Statistics (Forum) is an entity of the Cooperative System and, among its other activities, proposes principles of good practice to assist state and local education agencies in meeting this purpose. The Cooperative System and the Forum are supported in these endeavors by resources from NCES.

Publications of the Forum do not undergo the same formal review required for products of NCES. The information and opinions published here 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.

October 2020

This publication and other publications of the National Forum on Education Statistics may be found at the websites listed below.

The NCES Home Page address is http://nces.ed.gov

The NCES Publications and Products address is http://nces.ed.gov/pubsearch

The Forum Home Page address is http://nces.ed.gov/forum

This publication was prepared in part under Contract No. ED-IES-16-Q-0009 with Quality Information Partners, Inc. Mention of trade names, commercial products, or organizations does not imply endorsement by the U.S. government.

Suggested Citation

National Forum on Education Statistics. (2020). *Forum Guide to Cybersecurity: Safeguarding Your Data* (NFES 2020137). U.S. Department of Education. Washington, DC: National Center for Education Statistics.

Technical Contact

Ghedam Bairu

(202) 245-6644

ghedam.bairu@ed.gov

Foreword

The National Forum on Education Statistics (Forum) is pleased to present the *Forum Guide to Cybersecurity: Safeguarding Your Data*. The purpose of this document is to provide timely and useful best practice information to help education agencies proactively prepare for, appropriately mitigate, and responsibly recover from a cybersecurity incident. This resource reflects lessons learned by the education community and provides recommendations that will help agencies protect their systems and data before, during, and after a cybersecurity incident.

Education agencies are data-rich environments, making 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, business e-mail compromise, and denial of service (DoS) 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 a critical topic of importance for education agencies.

This document focuses on cybersecurity, with a specific emphasis on data, from the perspective of the education data community. This resource is not intended as a comprehensive cybersecurity prevention and protection plan, and not all aspects of cybersecurity incident response are addressed. Rather, this document focuses on key activities intended to minimize the likelihood of a cybersecurity incident and help education organizations respond if an incident occurs.

Publication Objectives

This resource provides best-practice information to help SEAs and LEAs before, during, and after a cybersecurity incident to

- build awareness about why cybersecurity is important to education agencies;
- help education organizations identify, mitigate, and protect against potential security risks, vulnerabilities, and threats;
- focus on how agencies can prepare for, mitigate, and recover from a cybersecurity incident; and
- identify solutions that will help agencies protect their systems and data before, during, and after an incident.

Intended Audience

This resource provides useful recommendations to education agencies for fulfilling their responsibilities to manage or use network-connected systems, including information and data systems. The information in this resource is intended to help 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.

Organization of This Resource

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

- **Chapter 1** defines cybersecurity and illustrates the extent of cybersecurity incidents, threats, and vulnerabilities.
- **Chapter 2** discusses planning activities and proactive measures that agencies can take before a cybersecurity incident to prevent an incident in the future.

- **Chapter 3** reviews measures that agencies can take when a cybersecurity incident has occurred to minimize the impact of the incident.
- **Chapter 4** describes response activities after a cybersecurity incident has occurred to restore systems and their data.
- **Chapter 5** presents case studies from SEAs and LEAs that have planned for or experienced a cybersecurity incident.
- **Appendix A** contains a checklist of tasks and activities to be undertaken before, during, and after a cybersecurity incident.
- **Appendix B** provides a sample list of federal and state resources on cybersecurity.

National Forum on Education Statistics

The work of the National Forum on Education Statistics (Forum) is a key aspect of the National Cooperative Education Statistics System (Cooperative System). The Cooperative System was established to produce and maintain, with the cooperation of the states, comparable and uniform education information and data that are useful for policymaking at the federal, state, and local levels. To assist in meeting this goal, the National Center for Education Statistics (NCES) within the Institute of Education Sciences (IES)—a part of the U.S. Department of Education (ED)—established the Forum to improve the collection, reporting, and use of elementary and secondary education statistics. The Forum includes approximately 120 representatives from state and local education agencies, the federal government, and other organizations with an interest in education data. The Forum deals with issues in education data policy, sponsors innovations in data collection and reporting, and provides technical assistance to improve state and local data systems.

Development of Forum Products

Members of the Forum establish working groups to develop guides in data-related areas of interest to federal, state, and local education agencies. They are assisted in this work by NCES, but the content comes from the collective experience of working group members who review all products iteratively throughout the development process. After the working group completes the content and reviews a document a final time, publications are subject to examination by members of the Forum standing committee that sponsors the project. Finally, Forum members review and formally vote to approve all documents prior to publication. NCES provides final review and approval prior to online publication. The information and opinions published in Forum products do not necessarily represent the policies or views of ED, IES, or NCES. Readers may modify, customize, or reproduce any or all parts of this document.

Working Group Members

This online publication was developed through the National Cooperative Education Statistics System and funded by the National Center for Education Statistics (NCES) within the Institute of Education Sciences (IES)—a part of the U.S. Department of Education (ED). The Cybersecurity Working Group of the National Forum on Education Statistics is responsible for the content.

Chair

Jay Pennington, Iowa Department of Education

Members

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)

Consultant

Elizabeth Lieutenant, Quality Information Partners

Project Officer

Ghedam Bairu, National Center for Education Statistics

Acknowledgments

The Cybersecurity Working Group would like to thank the Technology Committee of the National Forum on Education Statistics. The Committee's preliminary work to develop a white paper on the convergence of physical security, cybersecurity, and data security was instrumental to the formation of the Cybersecurity Working Group. The working group would especially like to thank Steven Hernandez (U.S. Department of Education), who shared comments and suggestions that improved this document. Members of the Cybersecurity Working Group would also like to thank everyone who reviewed or otherwise contributed to the development of the *Forum Guide to Cybersecurity: Safeguarding Your Data*, including the following

Reviewers

Shuwan Chiu, Illinois State Board of Education

DeDe Conner and Robert Hackworth, Kentucky Department of Education

Dan Dandurand, South Sioux City Community Schools (NE)

Dawn Gessel, Putnam County Schools (WV)

Kathi Grossenbacher, Kansas State Department of Education

Marilyn King, Bozeman School District #7 (MT)

Raymond Martin, Connecticut State Department of Education

Adrian L. Peoples, Delaware Department of Education

Steve Young, Washington State Office of Superintendent of Public Instruction

Case Study and Real-World Example Contributors

Bozeman School District #7 (MT)

Marilyn King, Deputy Superintendent Instruction

Indiana Department of Education

John Keller, Chief Technology Officer

Noblesville Schools (IN)

Andrew Swickheimer, Director of Technology

St. Louis Public Schools

Cheryl L. VanNoy, Deputy Superintendent, Accountability, Assessment, Technology Services, Students Records, & Data

Glossary of Common Terms

Bring Your Own Device (BYOD)–Policies that permit students to use their own mobile devices (for example, laptops, tablets, and cellphones) at school.

Business e-mail compromise (BEC)–Also known as e-mail account compromise (EAC), BEC is a form of online crime that exploits the use of personal and business e-mail. BEC scams target both organizations and people using a combination of phishing, social engineering, spoofing, or malware to negatively affect the targets.

Business continuity–An agency's ability to sustain mission-critical business processes during and after a significant disruption.

Containerization–Containerization isolates users' operations within an application virtually, minimizing access to data that are not being used directly.

Continuity of operations plan–A plan for restoring an agency's mission essential functions at an alternate site and performing those functions for up to 30 days before returning to normal operations.

Cross-site scripting (XSS)–XSS uses malicious script embedded in a web application (such as a compromised link in an e-mail message) to gather user data and, when executed, allows attackers to access sensitive user data.

Cybersecurity–The protection of network-connected systems and the data and information that are stored on, processed by, or transmitted by these systems from threats or security vulnerabilities.

Data breach–The intentional or unintentional release of secure information–including personal, sensitive, or confidential information–to an untrusted environment. Once released, information is vulnerable to being viewed, copied, transmitted, stolen, or used in an unauthorized manner.

Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks–A DoS or DDoS attack occurs when a server is deliberately overloaded to the extent that the website shuts down and is made inaccessible to legitimate users. A DoS attack uses one computer and one internet connection, while a DDoS attack uses multiple computers and internet connections.

Eavesdropping attack–When an attacker listens passively to authentication protocol to capture information that can be used in a subsequent active attack.

Encryption–The process of using a cryptographic algorithm (called cipher) to make information unreadable to anyone except those possessing special knowledge, usually referred to as an encryption/decryption key.

Internet of Things (IoT)–A rapidly evolving and expanding collection of interrelated and diverse technology devices that connect to a network or to one another and exchange data without necessarily requiring human-to-machine interaction.

Malware–Malicious software that is intentionally designed to damage a computer, device, server, client, or network.

Man-in-the-middle attack–When an attacker secretly intercepts or alters data or communications that are exchanged between two parties.

Network–A collection of interconnected components, such as routers, hubs, cabling, wireless devices, telecommunications controllers, key distribution centers, and technical control devices, that enable system implementation.

Phishing–Targeted communication in which an illegitimate sender poses as a legitimate business or organization and attempts to obtain personal or sensitive information from targets.

Ransomware–A form of malware that encrypts a user's system, device, or data and demands payment of a ransom for the user to regain access.

Scareware–A form of malware that uses social engineering to induce concern, anxiety, or fear in users, typically to manipulate users into buying unwanted software.

Spoofing–The use of a fake sending address, commonly an e-mail header or Internet Protocol (IP) address, to appear legitimate in an attempt to access a system and obtain personal or sensitive information from targets.

Social engineering–An attempt to trick or deceive someone into revealing sensitive information, obtaining unauthorized access, or committing fraud by associating with the person to gain confidence and trust.

Software–Programs, procedures, rules, documentation, and associated data that tell a computing device how to work.

SQL injections–SQL attacks exploit website security vulnerabilities, often by inputting malicious SQL statements into a web application form, to gain access to the website's operations.

System–A set of regularly interacting parts that interact, or are assembled, to form a unified whole and serve a common purpose. In a technology system, this refers to all hardware, software, networks, cables, devices, peripheral equipment, information, and data that comprise the system environment.

Tabletop exercise–Small-group discussions that walk through a scenario and the courses of action an agency or organization will need to take before, during, and after an emergency or incident to lessen the impact. These exercises help assess plans and resources, and facilitate understanding amongst key decisionmakers and stakeholders.

Threat landscape–The evolution of technology infrastructure, systems, and devices, coupled with the proliferation of cybersecurity threats and attacks.

Contents

Chapter 1: Cybersecurity in State and Local Education Agencies

This chapter defines cybersecurity and illustrates the extent of cybersecurity incidents, threats, and vulnerabilities in education agencies.

At 6:30 a.m. on a Saturday, your work cellphone rings. An analyst in your information technology (IT) department has called to let you know that your agency is currently experiencing a ransomware attack. The ransomware is spreading throughout your agency's networks and encrypting each system and device it infects. The hackers have requested $1.3 million in exchange for the encryption key. Every minute that your agency waits to act, you run the risk of permanently losing access to mission-critical systems and data. If you do not counteract the ransomware by Monday morning, your agency might be unable to run payroll, track attendance, or even unlock the network-connected electronic doors. Your staff need permission to start taking all of your agency's systems and devices offline, but first, you need to call the head of your agency to explain the situation. **How well is your agency prepared to respond to this attack?**

This is not a fictional incident, but a real-life example of a cybersecurity incident in a school district. To learn more about this incident, see the ransomware attack case study included in Chapter 5.

What is Cybersecurity?

In this resource, cybersecurity is defined as the protection of network-connected systems and the data and information that are stored on, processed by, or transmitted by these systems from threats or security vulnerabilities. In other words, cybersecurity is the protection of technology systems and networks—including all devices and tools connected to them—against intentional or unintentional attacks or exposure. Cybersecurity is neither limited to IT nor restricted to protecting data from criminal use. This resource emphasizes the importance of data in cybersecurity to enable a holistic, integrated

Any system or device that connects to the internet is considered "network-connected." This definition includes, but is not limited to

- IT systems
- Data systems
- Security systems
- Student information systems (SISs)
- Communication systems
- Desktop and laptop computers, tablets, smartphones, other computing devices
- Field monitoring devices
- Printers and peripheral devices
- Smart classroom/building devices

approach to the security of systems and the data associated with those systems. While cybersecurity shares many principles and practices associated with data security and data privacy, cybersecurity is a distinct concept.

Why Does Cybersecurity Matter?

Given the widespread use of network-connected systems and devices, security is an increasingly critical consideration in education agency operations, including the collection, management, and use of education data. State and local education agencies (SEAs and LEAs) use networked technology such as Internet Protocols (IPs) to better monitor infrastructure and facilities to enhance physical safety and security. This technology has lowered costs for SEAs and LEAs because it can reduce the need for routine in-person monitoring and encourage regular maintenance, which can minimize the need for major repairs. SEAs and LEAs use other technology solutions, policies, and procedures to protect against threats to information systems and the confidentiality of sensitive data. During the widespread disruption caused by the coronavirus disease (COVID-19) pandemic, many education agencies rapidly responded by switching to a remote working and learning model.

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

As technological innovation advances, threats increase. Organizations across every sector experience cybersecurity incidents, and education agencies are no exception. The frequency, severity, and impact of cybersecurity incidents in education agencies are increasing. Nearly three times as many cybersecurity incidents in K-12 education agencies were reported in 2019 than in 2018.[1] Schools and colleges were the second-highest targets of ransomware in 2019.[2] Education agencies need to protect network-connected systems, including IT and data systems, from cyber-attacks, data breaches, and other security threats. It is important for education agencies to act now to ensure they are protected.

> Cybersecurity incidents are increasing in education agencies. Nearly three times as many incidents were reported in K-12 agencies in 2019 than in 2018, and schools and colleges were the second-highest targets of ransomware in 2019.

There are many reasons why education agencies, especially LEAs, are targets for cybersecurity incidents:

1. Education agencies are data-rich environments and have access to detailed and sensitive student and staff data.
2. Agencies need to balance security against the access needs of staff and other stakeholders, which can increase vulnerabilities and risks.
3. Competing agency needs may be prioritized over cybersecurity.
4. Smaller districts can face many cybersecurity challenges, particularly when few technology staff are available to manage or mitigate threats.
5. High-profile attacks against education agencies often garner media coverage, which could influence agencies to pay off ransoms and minimize the chance of negative press.
6. Agencies have the resources to pay off ransoms, either from cybersecurity insurance or from budgeted funds allocated for other purposes.

1 Levin, D. A. (2020). *The State of K-12 Cybersecurity: 2019 Year in Review.* Retrieved March 9, 2020, from https://k12cybersecure.com/year-in-review/.

2 Sheridan, K. (2019, September 20). *Ransomware Strikes 49 School Districts & Colleges in 2019*. Retrieved March 9, 2020, from https://darkreading.com/threat-intelligence/ransomware-strikes-49-school-districts-and-colleges-in-2019/d/d-id/1335872.

Rapid innovation in the technology sector affects and reshapes nearly every aspect of society. Technology is used in education agencies to support student learning, agency decisionmaking, and organizational efficiency, as shown through the technology listed in figure 1. This figure presents various examples of common network-connected systems and devices that are used in various departments within an education agency; this figure is not an exhaustive representation of all technology that could be used in an agency. As with all network-connected systems and devices, each of the examples included in figure 1 can be compromised and used in a cyber attack against an education agency.

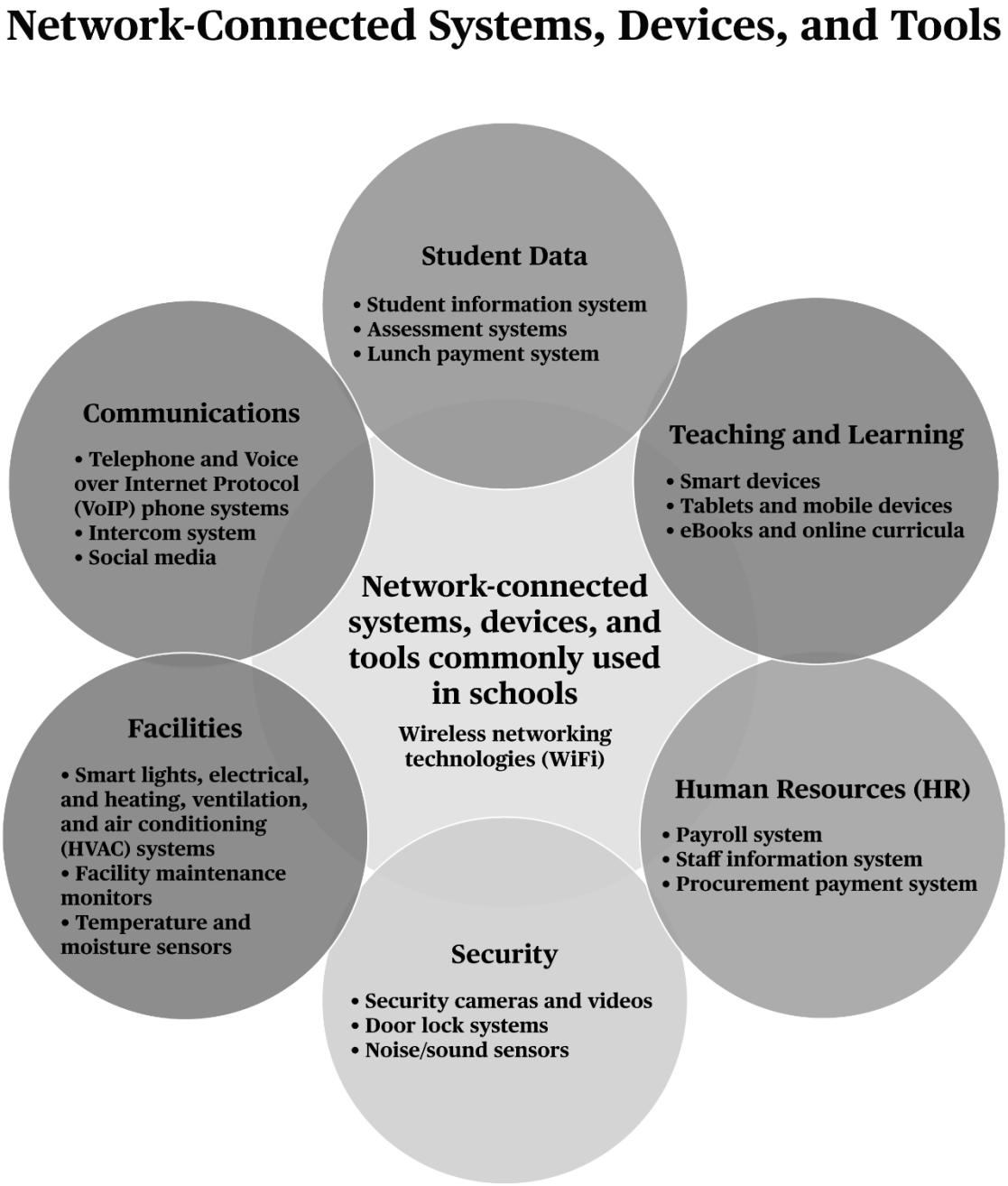


Figure 1. Examples of Network-Connected Systems and Devices Commonly Used in Schools

While technological advances enable new opportunities, they also introduce new threats. This may be exemplified best by the Internet of Things (IoT), which is composed of an evolving and expanding collection of interrelated and diverse technology devices that connect to a network or to one another and exchange data without necessarily requiring human-to-machine interaction. When unsecured IoT devices and systems are connected to agency networks, they can introduce new vulnerabilities and risks into a protected network environment. Bring your own device (BYOD) programs, paper and 3D printers, smart speakers and lights, and infrastructure monitoring devices (such as wind gauges and moisture monitors) may appear innocuous, but these devices can be exploited by attackers if they are not protected by cybersecurity best practices.

New threats also emerge at the intersection of physical security, cybersecurity, and data security. Networked components of physical security systems (cyber-physical security systems) and the emergence of the IoT present opportunities for safer facilities and schools. This convergence provides efficiencies and an expanded feature set to better manage both physical and cybersecurity. For example, internet-enabled devices have many convenient features such as

- automated safety notifications via text and e-mails;
- the ability to flexibly and easily add security cameras, sensors, and monitoring devices; and
- centrally managed automatic threat detection and response.

However, new technology also can create blind spots and vulnerabilities. New vulnerabilities and risks may include

- unauthorized local and wide area network (LAN and WAN) access to security devices;
- inadequate data protection policies and practices by staff, vendors, and service providers;
- staff prioritizing expedience and convenience over cybersecurity best practices;
- system patches and security updates that are not routinely and reliably applied;
- cloud service providers leaking information;
- systems and devices that are controlled, housed, or monitored off-site; and
- use of wireless networks for malicious purposes.

Network-connected utilities—water; electricity; lighting; heating, ventilation, and air conditioning (HVAC); and emergency response connections—are essential for continuity of operations, but are also susceptible to vulnerabilities. Even school security systems, such as surveillance cameras, are vulnerable to cybersecurity threats. Security systems now operate on the same wired and wireless networks using the same IPs as other network traffic. These formerly closed systems now depend on shared network infrastructure. Additionally, many devices are cloud-integrated or cloud-dependent by default. A malicious person or organization could, for example, hack into a surveillance camera system to spy on people in the facility, ascertain when parts of a building are most vulnerable, or disable the system to gain entry without being detected by security staff. These types of threats and vulnerabilities must be countered through a robust, integrated approach to cybersecurity.

Hackers, phishers, and spammers can disrupt education agency operations; compromise the confidentiality, safety, and integrity of important agency assets; and engender fear and mistrust in an educational community. When a cybersecurity incident occurs, education agencies need to be prepared to respond in a manner that quickly restores affected systems. Education agencies need to be proactive to protect their systems and data from threats, strengthen weaknesses and vulnerabilities, and plan for potential future incidents. These proactive measures will help minimize the likelihood of future incidents and help agencies respond in an appropriate and timely manner if an incident occurs.

Cybersecurity During Crises

It can be easy to overlook cybersecurity best practices when rapidly adjusting to high-pressure, stressful situations. During the widespread disruption caused by the coronavirus disease (COVID-19) pandemic in 2020, many education agencies focused on pressing matters such as ensuring continuity of learning and switching to remote working. Given the stress caused by the pandemic, identifying and processing cybersecurity threats may have been more difficult. During these types of stressful situations, taking time to ensure that security is not compromised can be helpful. Cybercriminals seek to exploit situations during times of confusion and distraction. Stay alert.

The best time to think about a crisis is well before it occurs. While the pandemic is a real-life example of organizations evolving rapidly to meet new requirements, education agencies will face new challenges in the future. Robust threat modeling including natural and human-made threats can be an effective way to identify organizational strengths and opportunities to improve.

Cybersecurity Incidents in K-12 Education Agencies

States have varying reporting and disclosure requirements for cybersecurity incidents, so determining how often SEAs, districts, and schools experience cybersecurity incidents can be difficult. Cybersecurity can be a sensitive topic; as a result, agencies may be reluctant to voluntarily disclose an incident due to the negative publicity such an incident can generate. As a result, any counts of publicly disclosed cybersecurity incidents likely are underreported and represent a subset of incidents experienced by districts and schools. Nevertheless, a review of publicly disclosed information can illustrate the extent of cybersecurity incidents.

K-12 Cybersecurity Incidents in 2019

During the calendar year 2019, the K-12 Cyber Incident Map cataloged 348 publicly disclosed cybersecurity incidents affecting public K-12 schools, districts, charter schools, and other public education agencies (including regional and state agencies) in 44 states. Nearly three times as many cybersecurity incidents were reported in 2019 than in 2018, when 122 incidents were reported. This rise or hike can likely be attributed to schools' increased technology use, cybercriminals' increased targeting of LEAs, vendor incidents that involved a number of LEAs, and greater awareness of and reporting about cybersecurity incidents.[3] Figure 2 shows that

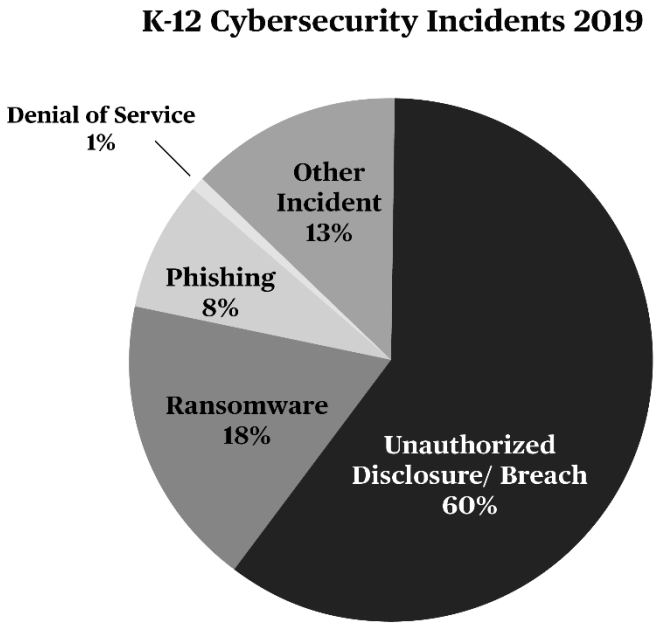


Figure 2. Cybersecurity Incidents by Type

NOTE: 348 total publicly disclosed cybersecurity incidents.

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

3 Levin, D. A. (2020). *The State of K-12 Cybersecurity: 2019 Year in Review.* Retrieved March 9, 2020, from https://k12cybersecure.com/year-in-review/.

data breaches were the most common type of K-12 cybersecurity incident reported during 2019, followed by ransomware, phishing attacks, and denial of service (DoS) attacks. Other types of reported incidents include malware and viruses, unauthorized access to systems, hacking and defacing school websites and social media, and attempted financial theft.

Cybersecurity incidents are not limited to a specific type of locality or setting. As shown in figure 3, between 2016 and 2019, nearly every state in the nation was affected by at least one publicly disclosed cybersecurity incident in a public K-12 education agency.

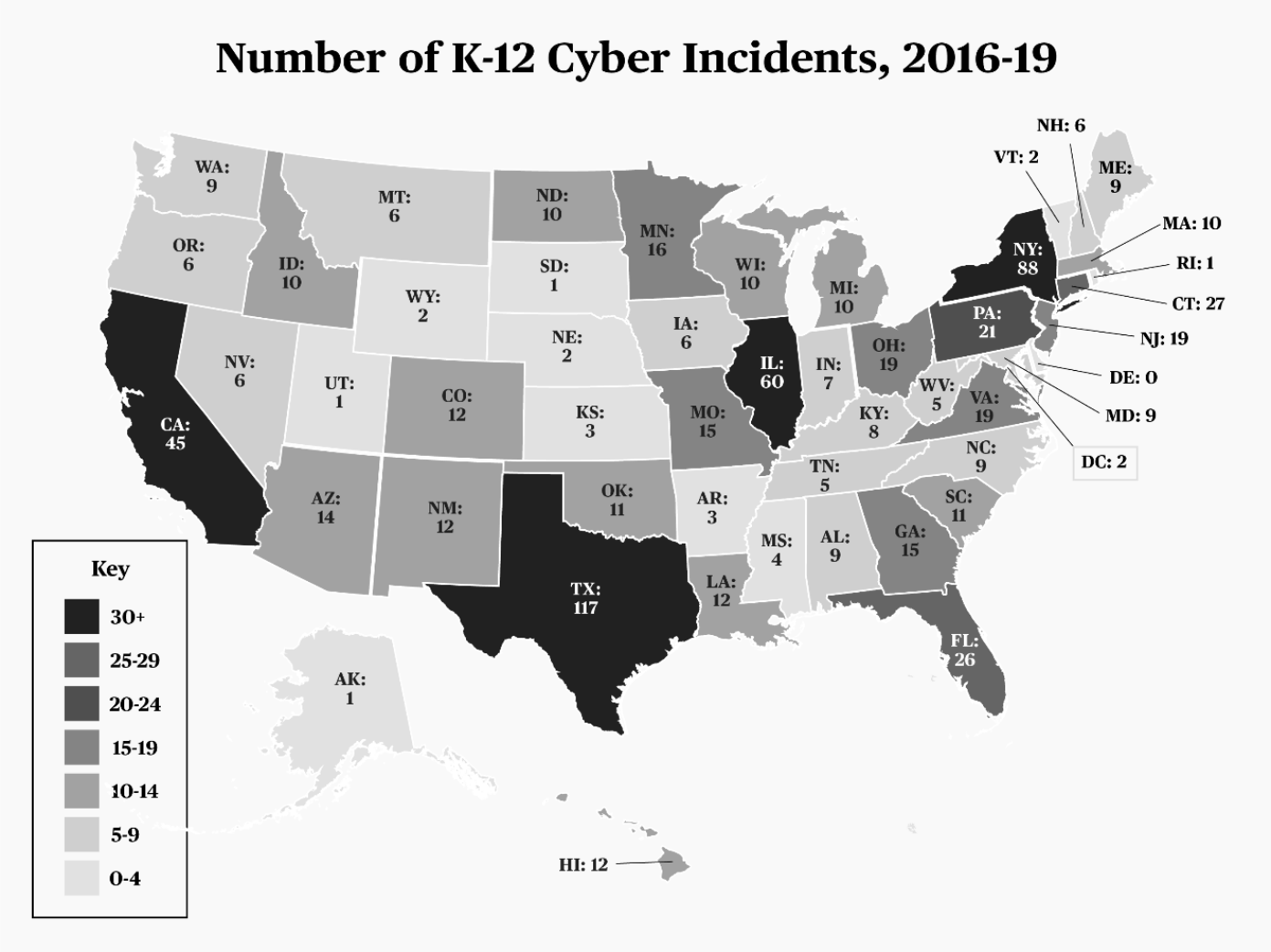


Figure 3. Cybersecurity Incidents by State

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

Types of Cybersecurity Threats and Vulnerabilities

Education agencies face a wide variety of cybersecurity threats and vulnerabilities. "Threat" refers to any circumstance or event with the potential to adversely affect agency operations (including mission, functions, image, or reputation), agency assets, people, or other organizations through a system via unauthorized access, destruction, disclosure, modification of information, or denial of service; vulnerability refers to weakness in a system, system security procedures, internal controls, or implementation that could be exploited by a threat source.[4]

The case studies presented in chapter 5 detail the actual experiences of SEAs and LEAs planning for and responding to cybersecurity attacks, threats, and vulnerabilities, including

- developing a data breach response protocol;
- implementing a cybersecurity program;
- responding to an SQL injection attack;
- responding to a vendor data breach; and
- recovering from a ransomware attack.

Even staff with in-depth cybersecurity knowledge can fall victim to common threats and vulnerabilities, like phishing e-mails and weak passwords. Common threats:

- **Data breach**–The intentional or unintentional release of secure information–including personal, sensitive, or confidential information–to an untrusted environment. Once released, information is vulnerable to being viewed, copied, transmitted, stolen, or used in an unauthorized manner. A data breach may originate from various sources:
    - Internal threats–Actors within an organization (for example, employees, contractors, and partners) who introduce risk through intentional or unintentional behaviors.
    - External threats–Actors who originate from outside of an organization (such as cybercriminals, attackers, or hackers), often with malicious intent.
    - Intentional breaches–Breaches that are motivated by intentionally malicious purposes.
    - Accidental breaches–Breaches that occur as a result of human error. For example, unintentionally providing public access to files or information, rather than limiting access to authorized people within an agency.
- **DoS and Distributed Denial of Service (DDoS) attacks**–A DoS or DDoS attack occurs when a server is deliberately overloaded to the extent that the website shuts down and is made inaccessible to legitimate users. A DoS attack uses one computer and one internet connection, while a DDoS attack uses multiple computers and internet connections.
- **Spoofing and phishing**–Both spoofing and phishing involve the use of fake communication, most commonly e-mail, to obtain personal or sensitive information. Spoofing is the use of a fake e-mail header or IP address to appear legitimate, while phishing is the use of targeted communication in which an illegitimate sender poses as a legitimate business or organization. Various phishing techniques can be used to obtain personal information from targets, including, but not limited to:
    - Spear phishing–A targeted attack on a specific person or organization that appears to originate from a colleague or acquaintance.

4 U.S. Department of Commerce, National Institute of Standards and Technology. (2017). *An Introduction to Information Security*. Retrieved January 8, 2020, from https://doi.org/10.6028/NIST.SP.800-12r1.

    - Short message service (SMS) phishing–An attack via text message.
    - Voice phishing (Vishing)–An attack via telephone.
    - Engine phishing–An attack via a fake website.
- **Malware, scareware, and ransomware**–Malware, or malicious software, is intentionally designed to damage a computer, device, server, client, or network. Scareware is a form of malware that uses social engineering to induce concern, anxiety, or fear, typically to manipulate users into buying unwanted software. Ransomware is a form of malware that encrypts a user's system, device, or data and demands payment of a ransom for the user to regain access.
- **Business e-mail compromise (BEC)**–Also known as e-mail account compromise (EAC), BEC is a form of online crime that exploits the use of personal and business e-mail. BEC scams target both organizations and people using a combination of phishing, social engineering, spoofing, or malware to negatively affect the targets.
- **SQL injections and cross-site scripting (XSS)**–SQL attacks exploit website security vulnerabilities, often by inputting malicious SQL statements into a web application form, to gain access to the website's operations. XSS uses malicious script embedded in a web application (such as a compromised link in an e-mail message) to gather user data and, when executed, allows attackers to access sensitive user data.
- **Man-in-the-middle and eavesdropping attacks**–Man-in-the-middle attacks are conducted by attackers who secretly intercept or alter data or communications that are exchanged between two parties. Eavesdropping attacks are when an attacker listens passively to authentication protocol to capture information that can be used in a subsequent active attack.
- **Password-related attacks and vulnerabilities**–Attackers can obtain passwords for malicious purposes through physical discovery, social engineering, network monitoring, malware, cracking, or guesses. Attackers sometimes share exposed passwords, credentials, and other sensitive data on the dark web. Passwords that use common phrases or are recorded in an unsecured environment are more vulnerable.
- **Software and operating system vulnerabilities**–Outdated or unpatched software can be vulnerable to cybersecurity threats. Systems and devices can also be more susceptible to threats when cybersecurity scanning and monitoring applications, such as antivirus software, are not used.
- **Infrastructure and facilities vulnerabilities**–Network-connected infrastructure and facilities systems can be vulnerable to cybersecurity threats. Not only do they provide an avenue for malware to be introduced, but they can also be hacked and then manipulated in ways that compromise operations. Cybersecurity vulnerabilities can also be introduced through lax physical security, such as an unlocked server room.
- **Removable media**–Removable media, such as thumb drives, external hard drives, and CDs or DVDs, can be lost or stolen, leaving the data stored on these devices susceptible to misuse. Corrupted removable media also could introduce malware into a secure device or network.

The following threat matrix (table 1) illustrates how the security of networked physical systems, IT systems, and data systems often overlaps.

Threat	Networked Physical Systems	IT Systems	Data Systems
Data breach via human error or intentional attack		√	√
DoS and DDoS attack		√	
Spoofing and phishing		√	√
Malware, scareware, and ransomware		√	√
BEC and EAC scams		√	√
SQL injections and XSS		√	√
Man-in-the-middle and eavesdropping		√	√
Password-related attacks and vulnerabilities	√	√	√
Software vulnerabilities that leave systems and data susceptible to attack	√	√	√
Unauthorized access to or cyberattack on physical facility systems (such as door locks, HVAC, security cameras, Voice over Internet Protocol (VoIP), public announcement, security alarms, fire/chemical/smoke alarms)	√	√	
Physical intrusion or forced entry to gain access to systems and data	√	√	√
Removable media and devices that are used for malicious purposes or store unsecured data		√	√

Table 1. Threat Matrix

The simplest cybersecurity measures can have a big impact, but may be easily overlooked. Sharing usernames and passwords is commonly acknowledged as inappropriate, yet staff still compromise system security with this frequent practice. For example, a staff member might leave their desk computer on for their colleagues to use during a meeting. While the staff member intended to be helpful, their action could leave any information stored on the computer vulnerable. If the staff member also happened to leave a sticky note on their monitor with the username and password for their agency's SIS, the agency could face serious consequences as a result of leaving student information susceptible to a data

breach. Furthermore, sharing access to secure data systems is considered a crime in certain jurisdictions. Remember, being helpful should not include compromising security.

Cybersecurity threats and vulnerabilities can manifest in different ways and cause varying levels of damage, as illustrated in table 2.

Threat/ Vulnerability	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
Infrastructure and facilities vulnerabilities	• Fire alarms triggered to evacuate school puts students exiting the building at risk or provides malicious actors with access to an unsecured building • Hacked VOIP systems allow malicious actors to steal information, eavesdrop on conversations, or place fraudulent calls • Hacked food service systems reveal student/family financial information • Hacked HVAC systems result in unhealthy temperatures that lead to school closures

Table 2. Potential Consequences of Cybersecurity Threats and Vulnerabilities

While cybersecurity threats are perceived as originating outside of the education community, insiders also can be a source. After all, staff may unintentionally put their agency at risk by sharing passwords, storing passwords in browsers, leaving applications or data systems open and unmonitored, publicizing their vacation schedules, or other seemingly innocuous actions that can be exploited by malicious actors or unauthorized people. Threats can come from

- **criminal outsiders**–people who intentionally take advantage of security vulnerabilities for malicious purposes;
- **unintentional outsiders**–vendors, contractors, and other agency partners who compromise systems and data through lax security practices;
- **malicious insiders**–staff or students who intentionally compromise the security of a system or data; or
- **unintentional insiders**–staff or students who compromise security, even after receiving appropriate training.

Malicious Actors Capitalize on Major Events to Manipulate Targets

Malicious actors have exploited major events to target users' important information, as evidenced by the security threats that emerged during the coronavirus disease (COVID-19) pandemic.

- The U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency and the United Kingdom's National Cyber Security Centre issued a joint alert on April 8, 2020, about how malicious actors exploited the pandemic (https://www.us-cert.gov/ncas/alerts/aa20-099a). This alert provided an overview of COVID-19-related malicious cyber activity and offered practical advice that people and organizations could follow to reduce the risk of being affected.
- Phishing attempts, malicious websites, malware, ransomware, and shadow IT solutions increased as attackers targeted remote workers, many of whom were working from home for the first time. Teleconferencing services were vulnerable to attacks and scams, particularly services that were popular or new to the market. Malware distribution, such as spoofed messages from a user's IT department prompting users to install new software, also was observed.
- Malicious actors launched phishing campaigns and created fake websites to capitalize on public interest in the pandemic and make targets take specific compromising actions. Attackers sent phishing messages about government stimulus payments, intending to steal sensitive user information through credential harvesting. Attackers also presented malware as COVID-19 outbreak tracking software.
- To appear trustworthy, malicious actors use spoofed information, like using the name of official health agencies and organizations or official titles, such as "Doctor." Malicious files and fake e-mails, text messages, and websites also used pandemic-related themes, such as "Federal government issues stimulus payments to help all citizens during COVID-19."

Chapter 2: Before a Cybersecurity Incident—Planning and Prevention

This chapter discusses planning activities and measures that agencies can take before a cybersecurity incident to prevent an incident in the future. Improving the cybersecurity preparedness of an education agency is a continuous, multi-year process. By starting small, agencies can build toward broader improvements in the future. The recommendations below are not listed in linear order or in order of importance; rather, they comprise a set of best practices that may occur concurrently or in sequential order. The information is general and not exhaustive. Agencies should adapt the information provided to meet their specific needs and requirements.

> Forum Guide to Technology Management in Education
> https://nces.ed.gov/forum/tec_intro.asp
>
> This resource is designed to help education agency staff understand and apply best practices for selecting and implementing technology to support teaching and learning in the classroom. It addresses the widespread use and integration of technology in modern education systems and focuses on technology governance and planning, technology implementation, integration, maintenance, support, training, privacy, security, and evaluation.

Identify the Risk Landscape

As explained in Chapter 1, cybersecurity risks increase as technological innovations advance. Identifying an education agency's risk landscape in relation to the threat landscape can provide a helpful starting point for understanding risks, counteracting threats, and minimizing vulnerabilities. This primarily involves developing a **comprehensive inventory** of all agency assets (including all systems, devices, and data). Network-connected facility technologies (for example, digital or magnetic keys; heating, ventilation, and air conditioning (HVAC) systems; power over ethernet; and automated lights) should also be included in the inventory. The development of an inventory often includes the following steps:

1. Record information on agency assets (systems, devices, and data), including each asset's purpose and function, current use, and identifying information.
2. Prioritize agency assets based on mission-critical operations and business process functionality.
3. Establish and enforce criteria for which people and departments may have access to agency assets.
4. Compile technical documentation for each asset's operations and restoration.

Implement High-Impact, Low-Cost Solutions

Improving an agency's cybersecurity posture does not require extensive resources or high costs. There are many high-impact, low-cost solutions that agencies can implement with minimal resources. Below is a list of cybersecurity best practices that can be implemented to better protect education agencies.

- Network Security
  - Develop a schedule to patch servers and network components.
  - Segment networks to separate systems and users.
  - Disable network access from unnecessary regions/countries.
  - Require virtual private network (VPN) use when accessing agency information on non-agency networks.
  - Inventory all network-connected systems and devices.
  - Conduct quarterly inventory reviews and updates.
  - Change the default password on Internet of Things (IoT) devices.
- Device Security
  - Encrypt hard drives.
  - Ensure all devices are equipped with disk encryption software, including laptops, tablets, and mobile devices.
  - Require enhanced authentication.
  - Keep all operating systems and software patched and up to date.
  - Use anti-virus applications and keep applications up to date.
  - Force anti-virus applications to scan all connected devices.
  - Disable .exe files from automatically executing on any connected device.
- Account Security
  - Remove or disable all unneeded accounts.
  - Follow the rule of least privilege for all users and accounts.
  - Remove local administrator permissions.
  - Minimize access by restricting access to only those with a legitimate need.
  - Do not create "master" accounts with administrator access to all systems.
  - Minimize the use of any "generic" accounts.
  - Do not share accounts.
  - Ensure account logging is enabled.
  - Promptly reassess or disable accounts as staff change duties or leave the agency.
- Password Security
  - Require passphrases that adhere to current National Institute of Standards and Technology (NIST) guidelines, which are available on the NIST website at https://www.nist.gov/topics/cybersecurity.
  - Require multi-factor authentication.
  - Never share passwords.
- Train all users annually on cybersecurity best practices.

The case study on implementing a cybersecurity program included in Chapter 5 details how a state education agency (SEA) took a leadership role in supporting local education agencies (LEAs).

There are many free cybersecurity resources to assist education agencies, including staff training materials and network scanning tools. Sample federal and state resources on cybersecurity are listed in Appendix B and the Reference List sections of this document. Education agencies can also collaborate on cybersecurity matters, as discussed in the textbox on cybersecurity in large and small education agencies.

Cybersecurity in Large and Small Education Agencies

Cybersecurity is important regardless of the size of an education agency, but the capacity to implement cybersecurity best practices may be markedly different. For example, while SEAs in large states and LEAs in metropolitan areas may have a technology department with multiple staff members with cybersecurity expertise, a small LEA may have only one staff member with part-time responsibility for the district's technology operations.

Small LEAs may benefit from collaborating with other LEAs, developing relationships with their SEA or state technology agency, or working with regional groups, such as Regional Educational Laboratories (RELs). SEAs can provide, for example, assistance and incentives to help LEAs improve their cybersecurity preparedness. Agencies can also participate in consortiums and other cooperative arrangements to enhance cybersecurity. These types of collaborations can help LEAs share resources and access expertise to increase their capacity to implement cybersecurity best practices.

Provide Training

User training is one of the most important measures an agency can take to minimize cybersecurity risk. Informed users have the power to combat threats, mitigate risks, and identify attacks. Cybersecurity training is not only important for information technology (IT) and data staff. Rather, all end-users of information and data systems need to receive cybersecurity training, including all staff and students.

Training for Staff

Regular training provides agency staff, including teachers, with the information and preparation necessary to support effective cybersecurity measures. Training will help staff understand an agency's cybersecurity response plan and will prepare staff to effectively implement the plan if an incident occurs. Cybersecurity training may address a wide range of issues, including how to identify and mitigate threats, how to minimize the likelihood of an incident, and what to do when an incident has occurred. Training should also review administrative policies and protocols for cybersecurity, which will help staff understand how to follow agency requirements. Cybersecurity training for all state employees is required in several states, and voluntary in most other states.[5]

Forum Guide to Education Data Privacy
https://nces.ed.gov/forum/pub_2016096.asp

This resource provides SEAs and LEAs with best practice information to use in assisting school staff in protecting the confidentiality of student data in instructional and administrative practices. SEAs and LEAs may also find the guide useful in developing privacy programs and related professional development programs.

Response training can range from a simple tabletop exercise to a full-scale simulation. Many cybersecurity training resources are available to help education agencies, including those developed by the U.S. Department of Education (ED), Student Privacy Policy Office (SPPO), and

5 National Conference of State Legislatures. (2017). *State Cybersecurity Training for State Employees*. Retrieved June 22, 2020, from https://www.ncsl.org/ncsl-in-dc/standing-committees/law-criminal-justice-and-public-safety/state-cybersecurity-training-for-state-employees.aspx

Privacy Technical Assistance Center (PTAC). Sample training resources are listed in Appendix B and the Reference List sections of this document. Common training topics:

- **Risk assessment**—How to identify potential threats, including the probability of occurrence and the estimated cost of potential losses, and points of vulnerability within the agency.
- **Protecting private and personally identifiable information (PII)**—How to conform to privacy policies and legislation using techniques and practices such as disclosure avoidance, limitation, and redaction.
- **Spoofing, phishing, viruses, spyware**—How to identify, report, and neutralize common cybersecurity threats that affect education agencies.
- **Identity and access control**—How to protect files, encrypt transmissions and files, set permissions, and authenticate users.
- **Physical security**—How to secure and prevent unauthorized access to physical facilities, resources, and assets.
- **Security best practices for common technology applications (internet, e-mail, student information systems [SISs])**—How to use common applications safely and responsibly, per agency policy.
- **Incident response protocols**—How to proceed in the event of an incident, in keeping with an agency's cybersecurity response plan.

A best practice is to require users to participate in training and also demonstrate that they understand the related risk mitigation practice through an assessment. The "Digital Drivers' License" model can be extended so that students and staff prove that they can responsibly and safely handle access to or management of physical, cyber, and data assets.

The convergence of network-connected physical, cyber, and data technology calls for adjustments to training and support to build capabilities and normalize practices that prevent, protect against, respond to, and recover from incidents. Table 3 identifies training topics that address the security of networked physical systems, IT systems, and data systems.

Training Topic	Networked Physical Systems	IT Systems	Data Systems
Data breach awareness		√	√
Training on protecting private information (Family Educational Rights and Privacy Act [FERPA], Health Insurance Portability and Accountability Act [HIPAA], Children's Online Privacy Protection Act [COPPA], state and local regulations)[6]			√
Phishing scheme training and audits		√	
Identity and access control security training and reminders	√	√	
Unauthorized entry prevention training including lock-down policies and procedures (training, audits, and drills)	√		
"Digital Drivers' License," that is, earning the right to use the network/systems		√	√

Table 3. Training Matrix

Training for Students

Students require different types of cybersecurity preparation than what is provided by staff training. Schools that apply for discounts on internet access or internal connections through the Federal Communications Commission's E-Rate program must certify their compliance with the Children's Internet Protection Act (CIPA) requirements regarding internet safety policies and technology protection measures. This includes educating minors about appropriate online behavior, including interacting with other people on social networking websites and in chat rooms, and cyberbullying awareness and response.

Many schools require students, parents, guardians, or a combination to sign acceptable use or responsible use policies for technology, which explain students' responsibilities for the use of school and district computing resources. These policies help students understand how to be responsible users of school-provided tools. In addition to school policies, teachers and staff can help model cybersecurity best-practices for their students.

States, districts, and schools adopt cybersecurity learning standards and curricula to prepare students to be responsible digital citizens in school and the workforce. The Daviess County Public Schools district, for example, requires 6- through 12-grade students to complete a grade-specific lesson on digital citizenship as part of the district's Digital Drivers' License program (https://sites.google.com/daviess.kyschools.us/dcpsdigcit/home).

6 For more information on FERPA and HIPAA, see the J*oint Guidance on the Application of the Family Educational Rights and Privacy Act (FERPA) and the Health Insurance Portability and Accountability Act of 1996 (HIPAA) to Student Health Records*: https://studentprivacy.ed.gov/resources/joint-guidance-application-ferpa-and-hipaa-student-health-records.

Remote Learning

Many education agencies rapidly transitioned to remote working and learning during the coronavirus disease (COVID-19) pandemic. This presented new challenges on many fronts, including keeping virtual learning environments secure. The following strategies can help protect agency assets when students, families, teachers, and instructional staff are learning and working remotely.

- Conduct due diligence in reviewing remote learning products and services for robust cybersecurity features.
- Use remote learning technologies, such as a learning management system, that can support secure digital classrooms and communication channels with specific roles and permission limits for teachers and students.
- Provide teachers and instructional staff with a list of approved remote learning products and services.
- Establish best practices for student and staff use of remote learning technologies.
- Train teachers and staff to follow student privacy policies and best practices when working with student data at home or contacting students while others are present in the home.
- Monitor and guide student interactions to ensure that only appropriate content is posted and shared.
- Enable a firewall and access control to limit access to remote learning technologies and protect against unauthorized access.
- Ensure that laptops and other devices, such as mobile hotspots, provided to students are controlled and filtered per cybersecurity policies and requirements, including CIPA.
- Understand that there is less control over user access when students and staff use personal devices to access systems and resources remotely.

Sample cybersecurity and remote learning resources are listed in Appendix B and the Reference List sections of this document.

Secure Agency Networks

A network is a collection of interconnected components, such as routers, hubs, cabling, wireless devices, telecommunications controllers, key distribution centers, and technical control devices, that enable system implementation. Network security mechanisms monitor and prevent unauthorized access, misuse, modification, or denial of the information system and network resources. These mechanisms can also scan networks for vulnerabilities and automatically generate reports about how to improve network security. When correctly configured, a secure network perimeter will protect the systems, devices, and data on an agency's locally managed and operated side of the network from the public side of the network. Perimeter security mechanisms may include, for example, a firewall and an intrusion detection system. Regularly reviewing both cloud networks and local networks for potential risks is a best practice. Cloud service providers and agencies share responsibility for ensuring the security of services and data.[7] Software as a service (SaaS) allows users to connect to and use cloud-based apps over the internet. For these types of applications, the security burden is on the SaaS provider, but agencies should ensure that the SaaS is configured to meet agency requirements.

7 U.S. Department of Commerce, National Institute of Standards and Technology. (2012). *Cloud Computing Synopsis and Recommendations*. Retrieved April 24, 2020, from https://doi.org/10.6028/NIST.SP.800-146.

Segmenting a network is an effective strategy to prevent unauthorized access to and movement within an internal network. Segmentation divides a network into sub-networks (segments) of systems and devices that share similar purposes, functionalities, and security requirements. Properly configured and segmented networks can minimize the potential impact of a cybersecurity incident by making critical systems, devices, and sensitive information and data difficult to access. For example, if an agency provides wireless internet access to guests, the guest Wi-Fi network should be segmented and isolated from the agency's other networks to increase security. Network penetration tests also can strengthen network security. These tests target and subject systems and users to attacks that mimic those used by real-world attackers. Agencies then can secure any network weaknesses identified by the tests.

Remote Working

Many education agencies rapidly transitioned to remote working and learning during the coronavirus disease (COVID-19) pandemic. This presented new challenges on many fronts, including keeping agency networks, systems, information, and data secure. The following strategies and tools can help protect agency assets when staff are working remotely.

- Train all staff on cybersecurity for remote working.
- Provide staff with agency-supplied laptops and devices, such as mobile hotspots.
- Create and deploy privileged access workstations.
- Properly configure, patch, and secure remote desktops.
- Encrypt all agency-supplied desktops and laptops.
- Require virtual private network use or secure cloud/web-based solutions when accessing agency systems, information, and data.
- Password-protect all hardware, servers, and systems, and enable multi-factor authentication when possible.
- Enable multi-factor authentication for all agency accounts.
- Update software routinely.
- Turn on content filtering to restrict user access to potentially malicious or inappropriate content.
- Use secure communication and collaboration platforms.

If staff members use personal devices to access agency information and data, enable containerization and delete any local copies as soon as possible.

Assess Existing Systems

Continuous changes and innovations in technology underscore the importance of maintaining a proactive approach to cybersecurity. Cybersecurity attacks are sometimes planned months in advance. Minor problems or issues in system operability may indicate an impending attack and should not be ignored.

Regular security assessments can identify which systems are most critical to agency operations, which have sensitive data that must be protected, and which technologies are required for each system to operate. Assessments also uncover potential system vulnerabilities. Systems

assessment should be an ongoing part of agency operations. The findings from a cybersecurity self-assessment enable an agency to determine whether additional protective measures, system updates, or system replacements are needed. Many resources exist to assist agencies with the cybersecurity self-assessment process, including those developed by ED SPPO PTAC. In certain states, SEAs have developed resources to help LEAs conduct a self-assessment or have conducted cybersecurity audits for LEAs in their state. Sample self-assessment resources are listed in Appendix B and the Reference List sections of this document.

SEAs and LEAs may benefit from a coordinated approach to assessment because comparing separate assessment reports could uncover opportunities for efficiency and greater visibility of potential vulnerabilities. Agency stakeholders can participate in the self-assessment process—even students who are completing cybersecurity coursework can be engaged. To lessen the likelihood that information about the weakness of a system is shared, agencies can require stakeholders (such as students or contractors) who participate in the assessment process to sign a non-disclosure agreement (NDA). Hiring a third-party expert to conduct a cybersecurity assessment also can help. Agencies could consider system penetration tests, particularly for systems containing sensitive financial, student, or staff information. Penetration tests help agencies discover weaknesses in systems, ideally before malicious actors find and exploit them.

Many factors influence when and how agency systems are updated and replaced, including accountability requirements, statutes and legislation, funding availability, agency capabilities, and decisionmaker needs. Data systems, as well as the data, must be kept up to date due to the critical role of data in federal, state, and local decisionmaking. Maintaining the security and confidentiality of student and personnel data is crucial. As part of a system assessment, the timeliness and utility of data should be assessed; any data that are no longer needed would be candidates for destruction. Older systems may need to be retired and potentially replaced. Before retiring a system, the data within that system need to be migrated or destroyed. This will ensure that critical data and information are protected from unintended loss.

Monitor and Automate Security

Automated tools and software can help agencies identify potential threats and protect against incidents. Automated scanning and monitoring tools (such as antivirus, anti-spyware, and firewalls) identify and defend against potential threats. These tools can continuously and automatically test systems and network traffic for malware, monitor for physical intrusion and vulnerabilities, and monitor access to and use of sensitive data. They can also generate automated notifications for a wide range of security issues, most commonly when users log in to their account from a new device. These types of notifications can be enabled for other purposes, such as when users are granted control-level access, when users' personal identity management information is updated, and when irregular building or account access is detected.

Automatic protections (for example, automated reports and real-time backups, such as offsite backups, cloud storage, or a data warehouse) can be leveraged for security to minimize the loss of critical data in the event of a data breach or other security incident. Automated cloud storage backups are useful in the case of a physical security breach. These backups can be a critical source of data if a cybersecurity incident affects agency data, thereby enabling agency operations to resume promptly. However, automated backups must also be protected from cybersecurity threats. Automated backup systems with rigorous cybersecurity protections can help defend against threats.

A Certified Ethical Hacker (CEH), also known as a "white hat" hacker, can complement an agency's automated security tools. CEHs are skilled professionals who understand system security and can identify system weaknesses and vulnerabilities that are not identified through

automated processes. SEAs and LEAs could leverage assessments and technical services offered by the U.S. Department of Homeland Security (DHS), Cybersecurity and Infrastructure Security Agency (CISA), including the cyber hygiene program. This program helps secure internet-facing systems from weak configuration and known vulnerabilities, and encourages the adoption of modern security best practices. CISA performs regular network and vulnerability scans and delivers a weekly report for action. More information is available at https://us-cert.cisa.gov/resources/ncats.

Establish a Cybersecurity Response Plan

> The case study on developing a data breach response protocol included in chapter 5 details the experience of an LEA establishing a cybersecurity response plan.

Cybersecurity planning encompasses plans, policies, procedures, and activities to proactively prepare for, appropriately respond to, and responsibly recover from a cybersecurity incident. The plan includes all of an education agency's actions to protect systems and data before, during, and after a cybersecurity incident. This includes

- developing individual and organizational capability to manage risk and counter threats;
- implementing appropriate safeguards to protect systems, hardware, devices, and software;
- implementing tools and activities to identify the occurrence of an incident; and
- developing and maintaining plans for restoring any systems, hardware, devices, and software that may be affected by an incident.

A response plan that aligns with state and local planning efforts and legislation will help ensure the agency follows applicable policy. Some states, such as Washington, have established policies and processes for reporting cybersecurity incidents. In Washington, state agencies must report all IT security incidents to the State Chief Information Security Officer and the Security Operations Center located in the state's Consolidated Technology Services agency. Reported incidents are investigated and escalated when necessary.

Aligning cybersecurity plans with related agency planning and preparation activities can strengthen agency operations. Every organization should have a continuity of operations plan (COOP) and a business continuity plan (BCP), so cybersecurity response planning can be included in these plans. A COOP focuses on restoring an agency's mission-essential functions at an alternate site and performing those functions for as many as 30 days before returning to normal operations, while a BCP focuses on sustaining an agency's mission and business processes during and after a disruption.[8] Information on disaster recovery planning can be found in the *Forum Guide to Planning for, Collecting, and Managing Data About Students Displaced by a Crisis* (2019) (https://nces.ed.gov/forum/pub_2019163.asp).

A timely and efficient response plan is crucial because cybersecurity incidents require urgent response. A cybersecurity response plan typically includes

- specific actions that will be followed when an incident occurs;
- roles and responsibilities matrixes to document the types of issues that may arise and identify which staff are responsible for specific tasks;

8 U.S. Department of Commerce, National Institute of Standards and Technology. (2010). *Contingency Planning Guide for Federal Information Systems*. Retrieved December 23, 2019, from https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf.

- criteria for deciding if and when to shut down a system, service, and data exchange, as well as if and when to close a facility, school, or agency; and
- how an agency and staff will communicate in situations where e-mail, intranet, and other online systems are compromised by an incident.

Storing both paper and digital copies of the response plan can ensure accessibility if a cybersecurity incident occurs. Digital documents can be updated and sent to users in response to an incident, and paper documentation can be referenced even if system access is compromised or if network connectivity is offline.

An annual cycle to review, assess, and update the response plan will keep the plan current with agency operations, systems, and capabilities. Planning exercises can help ensure that the plan is well understood and can be implemented effectively in the event of an incident. Agencies can determine the frequency and scale of planning exercises after considering the costs and benefits, as well as any state or local requirements. When appropriate and feasible, coordination with relevant agencies, community partners, vendors, and utility providers can help assess the effectiveness of a plan. Engaging with law enforcement before an incident can be useful because certain cybersecurity incidents may be criminal in nature.

When possible, forming a cybersecurity response team can help strengthen agency preparedness. Teams help agencies better identify, mitigate, and protect against potential security risks, vulnerabilities, and threats. They also help agencies prepare and plan for how to mitigate and recover from a cybersecurity incident. Including team members from across functional groups or areas within the agency–including staff with expertise in safety and security, IT, data, instruction, facilities, communications, emergency management, legal services, human resources, finance, and administration–will enable a holistic, coordinated approach to cybersecurity. This coordination enables agencies to address overlaps and shared risks at the convergence of physical security, cybersecurity, and data security. Agency leadership is critically important when developing an effective response plan. Leadership support and participation in the planning process will help ensure that the plan is understood and can be executed if an incident occurs.

> Forum Guide to Data Governance
> https://nces.ed.gov/forum/pub_2020083.asp
>
> This resource provides timely and useful best practices, examples, and resources for agencies implementing or updating their data governance programs. This guide includes an overview of data governance; discusses effective data governance practices, structures, and essential elements; describes how to meet privacy and security requirements while also meeting data accessibility and sharing needs; and includes detailed case studies from education agencies in their data governance effort.

A strong data governance program will complement cybersecurity planning efforts. Security considerations should be integrated into all levels of a data governance program. Including cybersecurity response team members in data governance groups can increase communication and improve understanding of the relationships between cybersecurity, data security, and data governance.

Review Policies and Procedures

Agencies should review federal, state, and local regulations, statutes, policies, and procedures that address cybersecurity and related issues such as data security, privacy, and data retention. A strong working knowledge of current federal, state, and local policies and procedures will help ensure that agency policy and procedures align with federal, state, and local requirements. Sample federal and state resources on cybersecurity are listed in Appendix B and the Related Resources sections of this document.

Policies govern how agency staff interact with systems and data and set requirements to which non-agency staff (for example, vendors, researchers, and others) must conform. Agencies should adopt comprehensive security plans, protocols, and procedures, which should be reviewed and updated annually. Standard policies and procedures address many important agency operations, including:

- **Data collection**–Regularly review which data are collected and evaluate whether or not the data should continue to be collected to ensure that data collections are aligned with agency policies and procedures.
- **System and data access**–Establish criteria to clarify who may, and may not, have access to systems and the data within those systems.
- **Access monitoring**–Assign responsibility for monitoring system permissions, regularly monitor who has access, and revoke access when necessary.
- **Data retention**–Examine data retention policies to ensure that data are properly retained and destroyed.

In following the policies and procedures listed above, an annual review process of an agency's data practices may include the following steps:

1. Conduct a data audit.
2. Review the reason for collecting data.
3. Determine which data are mission-critical and necessary for agency operations.
4. Review which people within and outside of the agency have access to the data.
5. Restrict/revoke unnecessary access permissions.
6. Discontinue any unnecessary data collections.
7. Review, update, and implement data storage and retention policies.

Agencies could review current insurance policies and coverage for protection against potential loss in the event of a cybersecurity incident. Commercial general liability and property insurance policies do not traditionally cover cyber risks, which may necessitate the purchase of a separate policy. Cybersecurity insurance typically protects against a wide range of incidents, including data breaches, ransomware attacks, hacking, and denial of service attacks, and can help pay for associated damages and losses, such as costs arising from legal fees, financial losses, and other services necessary to restore systems and business functions. In addition to the private marketplace, districts and schools may be able to procure cybersecurity insurance through state agencies. In West Virginia, for example, all districts have cyber liability coverage through the West Virginia Board of Risk and Insurance Management. In addition to individual agency coverage, agencies may wish to develop a policy that vendors and partners have adequate cybersecurity insurance coverage. One consideration when buying cybersecurity insurance is how incident response and system and service recovery will occur. Policies may require agencies to yield control of the cybersecurity incident to the insurer or its agent for the incident to be covered, and agencies need to ensure that this is an acceptable business arrangement.

Account Security

Password and identity management, authentication, and access are critical components of security. Thus, planning coherent policies for identity management that cover both physical and digital environments can be useful. Select security strategies include passphrases (rather than or in addition to passwords); multi-factor authentication; short message service (SMS) or text verification; biometric, application, and token authentication; and enterprise password managers.

Regularly reviewing agency policies governing passwords and identity management can ensure that they incorporate advancements and innovations in security. Accounts with unnecessary elevated permissions, old accounts that are no longer used but have not been deactivated or deleted, and accounts that grant access to multiple systems are at risk of being exploited. Human resources (HR) staff are essential for establishing and enforcing account-related business processes because HR departments maintain authoritative information on the status of staff. For example, retired staff no longer require access to many agency systems, but may still need to receive tax documentation through an agency's payroll system.

Common practices include

- The principle of least privilege, which limits user access to only the data and systems that are necessary for legitimate purposes.
- Zero trust, a standard that users should not be trusted at any time, regardless of whether they operate within or outside of an organization.[9, 10]

In practice, this would mean that agency staff only have access to the data and systems that are needed to fulfill their primary job responsibilities and duties. All staff can help strengthen cybersecurity by following the principle of least privilege and abiding by agency policies and procedures regarding the security of network-connected devices. Even facilities staff play an important role in cybersecurity because of their power to authorize building and room access. Remember, if an attacker can gain physical access to a server or system, there is rarely any way to stop them from taking over.

Procurement and Contracts

The cost of rebuilding or replacing affected systems and devices can be far higher than the cost of preventative measures. Because of this, agencies could consider incorporating cybersecurity into procurement and purchasing processes. Strong procurement policies and processes can help minimize cybersecurity risk, protect critical data, and prepare agencies to respond if an incident occurs. Before a major incident, agencies could identify how finances might be allocated, familiarize staff with public works rules, and create a preferred vendor list. Building renovations can be an opportunity to focus on cybersecurity by, for example, including cybersecurity in requests for proposals (RFPs). Agencies may also consider the purchase of a retainer for expert forensics services.

Many LEAs and SEAs work with vendors who manage portions of their agency's systems, such as an SIS. Therefore, contract negotiations and documents are crucial for clarifying system security responsibilities and requirements. Contracts should

- specify who owns the system and any data that are stored on, processed by, or transmitted by the system;
- outline specific system protection, risk minimization, and incident response requirements;
- specify which staff and vendors may access the system and for which purposes; and
- assign responsibility for the notification, mitigation, and resolution of any cybersecurity incidents that may occur.

9 American Council for Technology and Industry Advisory Council. (n.d.). *Zero Trust Cybersecurity*. Retrieved July 27, 2020, from https://www.actiac.org/hot-topics/zero-trust-cybersecurity.

10 U.S. Department of Commerce, National Institute of Standards and Technology. (2020). *Zero Trust Architecture*. Retrieved August 26, 2020, from from https://csrc.nist.gov/publications/detail/sp/800-207/final.

Agencies can reference industry and federal standards when building vendor security requirements, such as the NIST Special Publication 800-53 database: https://nvd.nist.gov/800-53. The Student Data Privacy Consortium Resource Registry includes a database with student data privacy agreement information from across the nation: https://sdpc.a4l.org/search_national.php.

Checklist of Actions to Perform Before a Cybersecurity Incident

- ✓ Develop a comprehensive inventory of all network-connected assets.
- ✓ Implement high-impact, low-cost solutions to secure networks, devices, accounts, and passwords.
- ✓ Provide regular training for all end-users of network-connected systems, including students.
- ✓ Secure agency networks, properly configure and segment agency networks, and establish a secure network perimeter.
- ✓ Conduct regular security, systems, and data assessments in a coordinated fashion with stakeholder participation.
- ✓ Consider hiring a third-party expert or Certified Ethical Hacker to assess agency security.
- ✓ Use assessment results to determine whether any systems need to be updated or replaced and whether any data need to be migrated or destroyed.
- ✓ Enable automated tools and software to identify potential vulnerabilities and protect against threats.
- ✓ Establish a cybersecurity response plan that will be followed when an incident occurs.
- ✓ Align cybersecurity planning activities with related planning and preparation activities.
- ✓ Form a cybersecurity response team and include members from across the agency.
- ✓ Ensure agency leadership understands and supports the response plan.
- ✓ Coordinate with relevant agencies, community partners, vendors, and utility providers, when appropriate.
- ✓ Proactively review federal, state, and local policies and procedures.
- ✓ Adopt comprehensive security plans, protocols, and procedures.
- ✓ Regularly review which data should be collected, and which should not.
- ✓ Set criteria for who may, and may not, have access to systems and data.
- ✓ Assign responsibility for monitoring system permissions, regularly monitor who has access, and revoke access when necessary.
- ✓ Examine data retention policies to ensure that data are properly retained and destroyed.
- ✓ Review current insurance policies and coverage for cybersecurity incident protection.
- ✓ Create coherent policies for identity management and passwords.
- ✓ Follow the principle of least privilege.
- ✓ Incorporate cybersecurity into procurement and purchasing processes.
- ✓ Consider the purchase of a retainer for expert forensics services.
- ✓ Review vendor contracts for cybersecurity requirements and responsibilities.

Chapter 3: During a Cybersecurity Incident—Mitigation

This chapter reviews measures that agencies can take when a cybersecurity incident has occurred to mitigate the impact of the incident. Many of the recommendations included in this chapter assume that the agency has adhered to the recommendations in Chapter 2 regarding adequate planning before a cybersecurity incident. The recommendations below are not listed in linear order or order of importance; rather, they are best practices that may occur concurrently or in sequential order. The information is general in nature and not exhaustive. Agencies should adapt the information provided to meet their specific needs and requirements.

Confirm the Incident

A cybersecurity incident might be detected through automated monitoring software or the observation of suspicious activity. As part of the cybersecurity incident response plan, agencies should have a process in place for staff to report a potential cybersecurity incident or event to the specific department or staff that are responsible for confirming whether an incident has occurred. After staff have reported the suspected incident, the department or staff identified in the cybersecurity response plan are to examine the available evidence and information for confirmation that an incident occurred and whether the incident is ongoing. Following incident confirmation, determine

- the scope and severity of the incident;
- the number of systems, devices, and users that have been affected by the incident;
- whether any data may have been compromised, and if so, the sensitivity of the data;
- the potential effect of the incident on routine agency operations; and
- whether the incident appears to be malicious or unintentional.

This information will enable the agency to respond appropriately. For example, an agency may need to initiate an advanced, agency-wide response if a malicious hacker attacked the agency's human resources system and accessed banking information. Conversely, if a staff member unintentionally accessed the agency's student information system under another staff member's log-in, the incident would not require an agency-wide response. Rather, the incident could be resolved through one-on-one corrective action and staff training.

Initiate a Response

Once a cybersecurity incident has been confirmed, the cybersecurity response team should consult the response plan to determine how to proceed. Depending on the scope and severity of the incident, some or all of the activities in the cybersecurity response plan may be activated. As noted previously, a malicious attack on an agency's mission-critical systems and data would

require a more advanced response than a minor, unintentional error that did not compromise agency operations. Response activities are intended to contain the incident and prevent further damage. This may include shutting down systems, unplugging devices, and resetting log-ins. Data management and systems operations may be disrupted, including, in extreme situations, the loss of hardware that houses a critical data system—although good planning should ensure that adequate backups are available. Prioritizing essential business functions can help focus response efforts on critical systems- and data-related tasks.

Maintain Communication

> The case study on responding to a vendor data breach included in Chapter 5 details the experience of an LEA maintaining communication during the incident.

Compromised systems can make communication difficult in the wake of an incident. E-mail, internet, and Voice over Internet Protocol (VoIP) systems may be inaccessible as a result of the incident, or they may be offline to help mitigate further issues. If regular telecommunication, internet, e-mail, and other communication channels are impacted by the incident, alternate or temporary communication methods may need to be used.

Depending on the severity of the incident, an agency's cybersecurity insurance provider might need to be contacted shortly after an incident occurs to ensure the agency responds per policy requirements. The team should also consult legal personnel to determine the agency's responsibilities and requirements regarding applicable legislation, regulations, and policies.

Communication with federal, state, and local law enforcement during and immediately following a cybersecurity incident may be appropriate if criminal activity is suspected. The U.S. Department of Justice, Computer Crime and Intellectual Property Section maintains a webpage with information and resources on reporting computer, internet-related, or intellectual property crime to federal investigative law enforcement agencies: https://www.justice.gov/criminal-ccips/reporting-computer-internet-related-or-intellectual-property-crime. If a financial crime is suspected, the U.S. Secret Service may be able to provide investigative assistance: https://www.secretservice.gov/investigation/#cyber.

External Communication

> The case study on responding to an SQL injection attack included in Chapter 5 details the experience of an SEA confirming the incident, initiating a response, and assessing affected systems.

Staff who are responsible for agency communications are often best-suited to coordinate external communications with parents, the media, and other parties. Stakeholders, particularly parents, often seek reassurance from agency leaders and want to know that the agency is aware of an incident and working to mitigate it. Communicating factual information about the incident in a timely, concise, clear, and frequent manner can help alleviate stakeholder concerns.

Teleconferencing Services

Teleconferencing services enable education agency staff to connect with their colleagues and students, but these services also introduce new risks. Many education agencies transitioned to remote working and learning during the coronavirus disease (COVID-19) pandemic. In response, malicious actors targeted teleconferencing service users, disrupted virtual meetings, spoofed legitimate meetings, and used fake websites and phishing e-mails to capture sensitive personal and financial information. The following teleconferencing best practices can help protect agencies, hosts, and users.

Agencies

- Look into different teleconferencing services and determine which ones meet agency security requirements.
- If a preferred service does not meet agency security requirements, consider working with the service to enhance security for potential future use.
- Ensure the services are configured appropriately and all passwords are protected.
- Enable multi-factor authentication for any accounts hosting meetings.
- Create policies for the secure use of teleconferencing service.
- Inform staff as to which services are approved and not approved.
- Train staff on how to use teleconferencing services safely and appropriately.
- Investigate any suspicious activity reported by meeting hosts and participants.

Meeting Hosts and Organizers

- Only use official, approved services.
- Make sure the administrator settings are correct.
- Require a password for entry. If sensitive information will be shared, consider sending attendees individual meeting passwords to verify their identity during the meeting.
- Use a lobby to only allow known attendees.
- Remove any participants who will not confirm their identity.
- Close or lock the conference after the meeting has started.
- Understand how to remove participants if needed.
- Limit what is shared on screen. Sharing files is safer than sharing applications and desktops.
- Be aware of what might be shown on a webcam. Blur, replace, or remove any sensitive information that might appear in the background.
- Inform participants whether or not screenshots are allowed.
- Keep a record of meeting attendees (such as phone numbers or Internet Protocol [IP] address). If a cybersecurity incident occurs, share this information with law enforcement.

Meeting Participants

- Double-check the web address of the meeting to ensure it is associated with the correct organization.
- Make sure teleconferencing software is up to date or join meetings via a web browser.
- Observe who is hosting and attending to confirm it is the correct meeting.
- Assume that everything shared during a meeting will be recorded and potentially made public.

Assess Affected Systems

Maintaining system integrity and security is of utmost importance. The first systems-related task for an agency that experiences a cybersecurity incident is to determine which systems have been affected and assess whether any data or information that are stored on, processed by, or transmitted by the affected systems have been compromised. This task is often completed as part of the incident confirmation process. Having an inventory of all agency assets (such as systems, devices, and data) will expedite this task. Log reports generated by automated monitoring software can help staff determine whether systems are working as they should be. If the threat remains active and has not been mitigated, any affected systems, hardware, devices, or software may need to be taken offline or shut down completely to prevent further impact. It can be helpful to prepare an alternate process, such as paper forms, for data collections that need to continue while systems are offline or otherwise inaccessible (for example, attendance, food services, mandatory testing). If an incident occurs during required federal or state data collections, an agency may need to request a waiver or extension.

If private or personally identifiable information (PII) has been exposed as a result of the incident, seek legal counsel's advice on informing data owners as soon as possible. PII includes, but is not necessarily limited to, direct identifiers (for example, names or identification numbers), indirect identifiers (such as birthdates), or other information that can be used to distinguish or trace a person's identity either directly or indirectly through linkages with other information. For a complete definition of PII specific to education records and for examples of other data elements that are defined to constitute PII, see the Family Educational Rights and Privacy Act (FERPA).

Checklist of Actions to Perform During a Cybersecurity Incident

- ✓ Report the suspected cybersecurity incident to the specific department/staff responsible for confirming whether an incident has occurred.
- ✓ Confirm that an incident has occurred by examining the available evidence and information.
- ✓ Determine the scope and severity of the incident to identify the impact.
- ✓ Consult the response plan to determine how to proceed.
- ✓ Prioritize essential business functions to help focus response efforts.
- ✓ Consider using alternate or temporary communication methods if regular communication channels are impacted.
- ✓ Contact the agency's cybersecurity insurance provider to ensure that response activities are per policy requirements.
- ✓ Consult legal personnel to determine the agency's responsibilities and requirements, including situations where PII has been exposed.
- ✓ Communicate the response plan to staff at all levels of the agency.
- ✓ Communicate the incident to law enforcement if criminal activity is suspected.
- ✓ Communicate facts about the incident to external stakeholders, including parents.
- ✓ Inventory all systems, determine which systems have been affected, and assess whether any data or information have been compromised.
- ✓ Prepare an alternate data collection process for any collections that must continue while systems are offline/inaccessible.
- ✓ Retrieve any lost data from an alternative source.

Chapter 4: After a Cybersecurity Incident—Recovery and Restoration

This chapter describes response activities to restore affected systems and data after a cybersecurity incident has occurred. In this resource, "after" a cybersecurity incident is defined as the time after the incident no longer poses an active threat. This period ends when all affected systems have been restored or replaced and the agency has resumed normal functionality. While the distinction between "during" and "after" a cybersecurity incident is relatively straightforward, the moment when such an incident had ended is not always clear. The endpoint may be more distinct in smaller incidents, but harder to identify in widespread incidents. In some cases, an infrequently used device or system that is infected may go undetected for some time, such as a system that is only used once per year for annual data reporting. The recommendations below are not listed in linear order or order of importance; rather, they are recommended best practices that may occur concurrently or in sequential order. The information is general in nature and not exhaustive. Agencies should adapt the information provided to meet their specific needs and requirements.

Investigate the Incident

An investigation will help determine the root cause of the incident, which enables an agency to implement strategies that will minimize the chance of future recurrence. Consult agency legal personnel for advice on how to proceed with an investigation. One important decision to be made when preparing for an investigation is whether to conduct an in-house investigation or solicit an external investigator or auditor. Important investigative matters include interviewing key personnel and locating, collecting, and preserving potential evidence.

For certain incidents, particularly those that may be criminal, evidence must be collected, analyzed, and preserved in a manner that ensures that the evidence is admissible in court. A computer forensics expert can help agencies with evidence collection and analysis. If criminal activity is suspected, be sure to coordinate with law enforcement on investigative matters. The U.S. Department of Justice, Computer Crime and Intellectual Property Section maintains a webpage with information and resources on reporting computer, internet-related, or intellectual property crime to federal investigative law enforcement agencies: https://www.justice.gov/criminal-ccips/reporting-computer-internet-related-or-intellectual-property-crime. If a financial crime is suspected, the U.S. Secret Service may be able to provide investigative assistance: https://www.secretservice.gov/investigation/#cyber.

Restore or Replace Affected Systems

> The case study on recovering from a ransomware attack included in chapter 5 details the experience of a local education agency (LEA) responding to and recovering from an attack.

System restoration is a component of implementing an agency's business continuity plan. Ideally, any affected systems will be quickly restored following a cybersecurity incident—good backups can certainly help. However, timely restoration is not always possible. Any systems directly affected by the incident may be inaccessible temporarily or permanently. Agencies should consider all available options for replacing, upgrading, restoring, and retiring any systems, hardware, devices, and software that were affected by the incident. At this stage, it can be helpful to consider the purpose and function of the system, the potential costs and benefits of restoration or replacement, and the security needs of the agency moving forward. Systems that are rebuilt or replaced can have stronger protections built in to better protect against cybersecurity threats and vulnerabilities.

If a critical system is offline or inaccessible for an extended period, local systems and routine processes may be strained. In this situation, a temporary application, system, or other alternative means of sharing information and data may be necessary. To be most effective, temporary systems should be developed and implemented quickly while ensuring that data are secure and confidentiality pledges are upheld. After a cybersecurity incident has been mitigated and any affected systems have been restored or replaced, agencies should formulate a plan to archive or destroy any temporary systems.

Major incidents that affect multiple systems for an extended period often incur significant expenses because of the costs of hardware, software, and labor. In certain cases, information technology (IT) staff will need support when recovering from a major incident. If additional staff are needed to aid in the recovery, agencies could consider temporarily reassigning staff, hiring new staff, or contracting with external groups (such as contractors, consultants, or vendors) to assist with recovery tasks such as inventory, data entry, and project management. Recovery activities could potentially be funded by cybersecurity insurance, reserve funds, infrastructure funding, or budget reallocations. Agency projects and priorities may also need to be adjusted following an incident.

Restore Affected Data

In the immediate aftermath of an incident, business operations and mission-critical functions (for example, heating, ventilation, and air conditioning (HVAC), payroll, and attendance) must be prioritized for business continuity. Given that certain data, such as student and personnel records, are necessary for a wide range of agency operations, it is also important to restore an agency's data and data-related functions following a cybersecurity incident. Any data and records that are lost temporarily or permanently as a result of a cybersecurity incident will need to be retrieved from an alternative source. An offsite backup, cloud storage, or data warehouse is often the first source; however, if backup data are not immediately accessible, an alternate source may have some, if not all, of the data. For example, a state education agency (SEA) data warehouse may be a source of some LEA data. Any temporary paper records that were used to collect data while systems were offline will need to be keyed in once the system is operational. Agencies may need to temporarily reassign staff or contract with a data entry service to assist with manual data entry. If any data were reported while systems were affected by the incident, those data should be audited for accuracy.

Evaluate the Response

When the cybersecurity response has concluded and routine agency operations have resumed, it is time to evaluate the adequacy and effectiveness of the cybersecurity response plan. All aspects of the response effort, including the response plan, staff actions, and agency systems, should be considered as part of the evaluation. The response team should also solicit feedback from all staff involved in or affected by the incident to determine the effectiveness of the plan. Reviewing the response plan in light of the agency's actual response will identify successful action items, as well as opportunities to improve.

Potential evaluation questions to be asked might include the following:

- Were the cybersecurity response planning activities adequate for the incident?
- What additional planning activities might have been helpful?
- Did the cybersecurity response team perform all of its necessary functions?
- Did the response team have adequate authority and preparation to complete the specific roles, duties, and responsibilities assigned to it in the cybersecurity response plan?
- Should new cybersecurity measures be used to automatically identify and mitigate potential future threats? If so, which tools, software, and protections should be implemented?
- Did agency policies and procedures help or hinder the response?
- Did the investigation reveal any shortcomings in the agency's cybersecurity practices?
- How effective was communication, both within and outside of the agency?
- What steps were taken to ensure data privacy during and following the incident?
- Was the confidentiality of all student data protected?
- Are there any long-term consequences of the cybersecurity incident that need to be addressed or explained, such as lost or incomplete data?
- What changes to the response plan should be implemented immediately, and what changes should occur after the next system replacement or upgrade?
- What other lessons can be learned from the incident and response?

The evaluation outcomes can be a catalyst for improved cybersecurity measures, such as increased training and more robust network security. Based on the evaluation results, the agency's business continuity plans, agency processes, and any affected systems should be reviewed and revised to strengthen future response efforts. Professional development and training materials should also be reviewed for potential preventative measures; subsequently, these materials should be updated to reflect any modifications to the response plan and incorporate lessons learned from the incident.

Checklist of Actions to Perform After a Cybersecurity Incident

- ✓ Consult legal counsel's advice on how to proceed with an investigation.
- ✓ Coordinate with law enforcement if criminal activity is suspected.
- ✓ Consider all available options for replacing, upgrading, restoring, and retiring any assets (such as systems, hardware, devices, or software) affected by the incident.
- ✓ Assess the purpose and function of the affected asset, the potential costs and benefits of restoration or replacement, and the security needs of the agency moving forward.
- ✓ Build stronger cybersecurity protections into any systems that are restored or replaced.
- ✓ Use a temporary application, system, or another alternative if necessary.
- ✓ Archive or destroy any temporary systems once they are no longer needed.
- ✓ Consider retaining staff support when recovering from a major incident.
- ✓ Identify funding sources to pay for recovery activities.
- ✓ Prioritize restoring an agency's business operations and mission-critical functions.
- ✓ Retrieve any lost data and records from an alternative source.
- ✓ Key in any data that were collected using temporary paper records.
- ✓ Audit any data that were submitted during the incident.
- ✓ Evaluate the adequacy and effectiveness of the cybersecurity response plan.
- ✓ Solicit feedback from staff to determine the effectiveness of the plan.
- ✓ Use the evaluation results as a catalyst for improved cybersecurity measures.
- ✓ Review and revise business continuity plans, agency processes, and any affected systems based on the evaluation results.
- ✓ Update professional development and training to incorporate preventative measures, response plan updates, and lessons learned.

Chapter 5: Case Studies from States and Districts

This chapter presents case studies that detail the actual experiences of state and local education agencies (SEAs and LEAs) concerning cybersecurity. They emphasize best practices and lessons that states, districts, and schools can learn from when developing or enhancing their cybersecurity practices. SEAs and LEAs that are planning to enhance their cybersecurity practices may find it useful to read about the experiences of other agencies.

The case studies are segmented into two sections:

- The first two case studies focus on planning and prevention activities that took place before a cybersecurity incident.
- The final three case studies focus on recovery and restoration activities that took place after a cybersecurity incident occurred.

In broad terms, the case studies include the following information:

- Overview of the agency's overall approach to cybersecurity.
- Descriptive statement of the cybersecurity threat, risk, or challenge that the agency experienced.
- Summary of the agency's experience addressing the cybersecurity threat, risk, or challenge.
- List of lessons learned based on the agency's experience.
- Checklist of best practices and helpful resources.

Some of the case studies also include overarching descriptive information on the agency.

Just as cybersecurity threats vary in their potential focus and impact, the methods and strategies featured in this chapter differ in multiple ways and are based on each agency's experience. Given that cybersecurity is ever-evolving, no single case study or group of related case studies will necessarily present a comprehensive solution to cybersecurity in education agencies. Successful methods for addressing cybersecurity will also vary based on state and local cybersecurity laws and policies. In all cases, appropriate internal experts—such as information technology (IT) staff, legal staff, and data staff—should be consulted to determine specific best practices for a particular agency.

Developing a Data Breach Response Protocol

Agency Overview

Bozeman School District #7 (BSD7), Montana, has 11 schools with a total student enrollment of approximately 7,000 and a total staff of approximately 800.[11] *Note: These numbers represent the most recent ED data and do not necessarily reflect the latest district data.*

Agency's Cybersecurity Approach

District leadership and staff observed many LEAs dealing with cybersecurity threats and attacks in recent years. As a result, the district was motivated to be proactive and develop a data breach protocol.

Cybersecurity Challenge

BSD7 has not experienced a major cybersecurity incident. When minor data breaches have occurred as a result of human error, they have been resolved. Although the district has not experienced a major data breach, the district recognized the importance of having a data breach response protocol in place. The district had protocols in place for other types of emergencies (such as a chemical spill or an earthquake) and wanted to set up a similar protocol to be used in the event of a data breach.

Agency's Experience

First, leadership and staff from across the agency—including Central Office administrators, the Technology Services Department supervisor and staff, and a school principal—met for an initial planning session. The group discussed various elements of a data breach response plan, including what information would be needed to develop a response, what tasks to do and when to do them, and which department should be responsible for completing certain tasks. Based on these discussions, the district developed a list of items that required further exploration and investigation. Members of the group conducted research online and talked to their professional networks to identify best practices for responding to a data breach. This work informed the development of the district's data breach protocol (DBP). The DBP includes specific tasks and activities to be undertaken in the event of a data breach, including

- collecting and reporting preliminary information on how the suspected data breach was identified;
- criteria for determining whether the breach has occurred and if so, the severity of the breach; and
- instructions and corrective actions on how to proceed, depending on the severity of the breach.

The group then met to review the DBP via an interactive tabletop exercise. These exercises consist of a series of slides that walk participants through an emergency scenario in chronological order. This allows participants to discuss their roles and responsibilities, decisionmaking processes, and responses during a particular type of emergency situation. The district has used tabletop exercises for a variety of emergency scenarios, such as armed intruder and active shooter scenarios. The DBP tabletop exercises typically last for 45 minutes and include the Technology Services Department, Central Office administrators and staff, and the district's School Resources Office. Bringing together different departments has helped participants understand who to communicate with if a data breach occurs.

11 U.S. Department of Education, National Center for Education Statistics, Common Core of Data (CCD), "Local Education Agency (School District) Universe Survey," 2018-19 v.1a; "Public Elementary/Secondary School Universe Survey," 2018-19 v.1a. Retrieved May 8, 2020, from http://nces.ed.gov/ccd/elsi.

The first DBP tabletop exercise identified several additional tasks to include in the DBP. For example, the exercise participants noted that it would be helpful to record how the breach was identified and that it was important to contact the district's liability insurance provider and disaster recovery contractor. This formative feedback was used to refine the DBP. As the district has engaged in subsequent tabletop exercises and strengthened the protocol, the district has established a solid plan for responding to a data breach.

In addition to the DBP, the district also has a letter template to notify the U.S. Department of Education (ED) if a data breach occurs, in keeping with ED best practices. In the event that a data breach occurs, the district will contact the ED Student Privacy Policy Office (SPPO) via phone, then follow-up with a formal letter. The letter template includes placeholders for information on the breach and actions taken by the district to mitigate the breach. While notifying the SPPO is voluntary, the district does so to make sure it is accountable for its actions and conducts a transparent response.

The district also has a data security tip sheet to help strengthen the district's security practices and minimize the risk of a breach. The tip sheet includes best practice information for staff on how to secure data when using district technology. It addresses the use of computers, writable media, e-mail, databases, cloud computing, and productivity and collaboration apps, as well as printed documents, passwords, and student information. The tip sheet was shared with the BSD7 Technology Steering Committee for review and input. The committee comprises primarily teachers, and their feedback was incorporated into the tip sheet, with the goal of providing concrete, helpful information for teachers to remember. To be easily accessible and digestible, the tip sheet can be printed on one double-sided sheet of paper. The tip sheet has been well received by both personnel and the public, and school officials have highlighted this resource as part of its commitment to data privacy and security.

Lessons Learned

- **Planning pays off**–In the event of a data breach, the DBP enables BSD7 to begin assigning responsibility for and working on tasks promptly and efficiently. The time spent on planning was valuable and considered well-spent by all.
- **Repeat reminders**– The BSD7 tip sheet helps remind agency personnel of best practices for data security. The tip sheet has received positive feedback from staff and administrators alike.
- **Timeliness is key**–A timely response is critical to containing a cybersecurity incident. By planning ahead, BSD7 will be able to quickly respond to a data breach.

Best Practices and Helpful Resources

- ✓ **Focus on the fundamentals**– Protecting student data is essential. Keeping this overarching goal in mind can help prioritize cyber and data security in agency operations.
- ✓ **Be prepared**–It is better to be prepared and never need to use an incident response plan than to experience an incident and not know what to do.
- ✓ **Assign responsibilities**–All tasks in a response plan need to be assigned to specific parties who will be responsible for the task's completion. Smaller agencies may be able to assign responsibilities to departments with just a few staff, while larger agencies with large departments may benefit from assigning responsibilities to specific people.
- ✓ **Keep the conversation going**–As systems and technology change, agency personnel need to be proactive and update security practices to protect agency systems and data from potential threats.

Implementing a Cybersecurity Program

Agency Overview

The Indiana Department of Education (IDOE) serves 1,919 public schools within 432 school districts with a total student enrollment of approximately 1,055,700 and a total FTE staff of approximately 143,600. *Note: These numbers represent the most recent ED data and do not necessarily reflect the latest state data.*[12]

Agency's Cybersecurity Approach

Indiana stakeholders recognized the need for attention to cybersecurity in schools. As part of the 2017 Indiana State Budget, IDOE received a $2 million appropriation from the Indiana Department of Homeland Security.

Cybersecurity Challenge

The appropriation was for IDOE to partner with a public research university in the state to provide assistance to IDOE and Indiana schools. An initial proposal for the partnership was projected to have a limited impact and was rejected. The funds were instead allocated to an IDOE-led program.

Agency's Experience

IDOE designed a multi-faceted cybersecurity program to improve the cybersecurity posture of Indiana K-12 education agencies and schools. The program components were informed by input from stakeholders and partner groups, including LEAs, the Indiana Chief Technology Officer (CTO) Council, and the Indiana Office of Technology. IDOE formally launched the program in May 2018 at an Indiana CTO Council event. The cybersecurity program aimed to have a broad impact that affected the awareness and professional capacity of educators in every district, as well as a deeper impact that provided funds to support districts in establishing managed security services. The program included five components:

- **Managed Security Services Grant**–This component provided matching grants of up to $25,000 for districts to contract with a reputable firm of the district's choosing for cybersecurity managed services. The grants were designed to encourage LEAs to prioritize cybersecurity funding and intended to provide 1:1 matching funds. Ultimately, the funding averaged 3:1, with LEAs providing $3 for every dollar provided by IDOE. The one-year grants were distributed in two rounds; 19 LEAs participated in the first round, and 12 LEAs participated in the second round.
- **Cybersecurity Task Force**–The task force was established in collaboration with the Indiana CTO Council to coordinate cybersecurity learning opportunities in the state. Members serve for a two-year term and meet at least two times a year, as well as attend conferences to support their own cybersecurity professional development. The task force serves as a consultative resource for IDOE and practitioners in the state and is encouraged to collaborate with non-technical staff, including superintendents, principals, and school business staff. The task force has developed a cybersecurity audit checklist, compiled best-practice information and resources, and also maintains a blog. Funds were available to support cybersecurity professional development at meetings and conferences held by other professional associations within the state, as well as task force member travel to state conferences and professional meetings.

12 U.S. Department of Education, National Center for Education Statistics, Common Core of Data (CCD), "Local Education Agency (School District) Universe Survey," 2018-19 v.1a; "Public Elementary/Secondary School Universe Survey," 2018-19 v.1a. Retrieved May 8, 2020, from http://nces.ed.gov/ccd/elsi.

- **Cybersecurity for Staff**–A preexisting contract for all state employees to receive security awareness training and a phishing simulation tool was expanded to include any LEAs that voluntarily wished to use the service, at no cost to the LEA. The awareness training included three mini-courses on cybersecurity basics. The phishing tool allowed administrators to develop and send phishing messages to staff and provided information on which staff clicked on unknown links. In the fall of 2018, 86 districts and more than 40,000 staff members were enrolled in the training. The service was extended for an additional year, and many LEAs continued to participate in the second year.
- **Cybersecurity for Students**–To encourage student interest in cybersecurity and related careers and help ensure a robust cybersecurity workforce and talent pipeline, IDOE sponsored district implementation of a high school cybersecurity course. LEAs received awards of up to $8,000 per school to assist in offsetting costs associated with implementing a cybersecurity course during the 2019-20 and 2020-21 school years. Seven LEAs participated in the first round of funding, and 51 LEAs participated in the second round.
- **Resource Hub**–This webpage provides a curated list of general cybersecurity resources to help district and school leaders. The Cybersecurity Task Force, K-12 technology leaders, and experts in the cybersecurity field helped identify resources for inclusion in the hub.

While the program was very well received by stakeholders, including participating LEAs and schools, it experienced several challenges. IDOE had anticipated that the managed security services grants and cybersecurity for staff training would have more participants. In addition, IDOE's request to the Indiana General Assembly for an additional round of funding was unsuccessful. Although funding was not renewed, the program has helped the state improve its cybersecurity preparedness. The program helped create the human infrastructure necessary to share cybersecurity information in a compelling and effective way. For example, in response to a rash of targeted attacks in fall 2019 against education agencies in other states, IDOE coordinated with the Cybersecurity Task Force to develop information that would help LEAs prepare themselves. In addition, a number of LEAs that received cybersecurity managed services grants have continued to contract for these services using their own funds.

As an example of the positive impact of the IDOE's work, Noblesville Schools (IN) has benefited from each aspect of the cybersecurity program. The district was awarded a $25,000 grant for one year of managed security services, which the district would have otherwise been unable to procure. This service helped the LEA identify current threats to its network, understand how to strengthen the network infrastructure, and close gaps in the network's security. After the grant ended, the LEA scaled back its managed security services contract to monitor its server environment, rather than the entire network, which would have been financially impractical.

The district also received a grant to cover the costs of the cybersecurity curriculum and teacher training. The district is currently teaching two sections of this course, which is helping students improve their cybersecurity preparedness. The district also uses the cybersecurity phishing tool. The district's use of this tool has had a measurable impact on the staff's ability to recognize and report phishing attempts. Since the district started using the phishing campaign tool, the pass rate has improved from 80 percent to 98 percent. The district plans to continue to use this tool quarterly, both to test current staff and to help new staff. Additionally, the LEA has availed itself of the cybersecurity resources, rubrics, and documents developed by the Cybersecurity Task Force.

The grants, tools, and resources provided by the IDOE cybersecurity program have demonstrably helped Noblesville Schools improve its cybersecurity preparedness. To help

spread the word to other LEAs in the state, Noblesville Schools has participated in IDOE-facilitated panel discussions at state conferences and meetings. This has helped other LEAs in the state learn about the IDOE program and allowed Noblesville Schools to share its experience.

Lessons Learned

- **Listen to stakeholders**—IDOE took the time to listen to Indiana LEAs, the Indiana CTO Council, and the Indiana Office of Technology before implementing the program. By reaching out to state stakeholders to understand their experiences, IDOE was better able to design a program that would meet stakeholder needs and solve challenges.
- **Align program components**—IDOE looked for ways to align this multipronged program to strengthen the program's efforts and impact. The resource hub, for example, was informed by the work and expertise of the Cybersecurity Task Force.
- **Seek out success**—IDOE considers the program a success even though funding for the program was not renewed. While quantifiable data on the program's impact is not available, LEAs who participated in the program have reported that they benefited from the SEA's efforts.

Best Practices and Helpful Resources

✓ **Be creative**—Don't let a lack of funding stand in the way of being proactive. Even without dedicated cybersecurity funding, SEAs can promote cybersecurity best practices, provide free information and resources, help negotiate lower rates for cybersecurity services, and amplify efforts by state stakeholders.

✓ **Don't limit yourself**—SEA support of LEA cybersecurity should not be contingent on the expertise or capacity of SEA staff. SEAs can play a critical role in coordinating, communicating, and supporting cybersecurity efforts within their state.

✓ **Helpful resources**—More information and free resources are available at https://www.doe.in.gov/cybersecurity:

- Cybersecurity Task Force Cyber Blog (https://www.indianactocouncil.org/domain/39).
- Resource Hub (https://www.doe.in.gov/cybersecurity/resource-hub).
- Indiana K-12 Cybersecurity Audit Checklist (https://docs.google.com/spreadsheets/d/11vdbs4_Eh8RohaOPH_V0ksmT37JzxsE4K_UWyc5WTaM/edit?usp=sharing).
- Indiana CTO Council (https://www.indianactocouncil.org/).

Responding to a SQL Injection Attack

Agency's Cybersecurity Approach

Several years ago, an unnamed SEA developed an agency-wide privacy incident response plan, which sets guidelines for responding to privacy incidents and data breaches that may result in the exposure of personally identifiable information (PII). The plan was informed by best-practice guidance, including resources from the U.S. Department of Education's Privacy Technical Assistance Center (PTAC) and the U.S. Department of Defense. It defines key terms, describes personnel roles and responsibilities, sets criteria for determining an incident's severity, and outlines steps personnel must take when an incident is suspected to have occurred. The plan was disseminated to key personnel in the agency, including staff in the information technology (IT) office. The IT team members are well qualified, dedicated, and work together to ensure the agency's systems are secure.

Cybersecurity Challenge

Approximately 18 to 24 months after the privacy incident response plan was developed, a data systems staff member noticed suspicious network activity. Servers located in Germany were being used to launch a SQL injection attack against one of the agency's websites that was previously used for data reporting.

Agency's Experience

The SQL injection attack was discovered within a day and managed quickly. Fortunately, the specific webpage that was targeted had not been used for several years and only contained e-mail addresses for an application that was no longer in use. IT staff shut down the website, confirmed that the SEA's servers were safe, and took precautions to limit cybersecurity vulnerabilities in the future. Immediately following the identification of the attack and for the next two weeks, the IT team diverted all its time to review every website the agency used for reporting data. Each website was taken offline, thoroughly reviewed, and then put back online with a proxy server in place to limit the likelihood of a future attack.

The privacy incident response plan helped inform the agency's response, particularly in facilitating staff communications. The plan ensured that key SEA staff were notified promptly, understood their roles and responsibilities, and involved appropriately in the response. In following the plan, for example, the agency investigator was involved in the response and notified the Federal Bureau of Investigation (FBI) of the incident.

Following the incident, the agency has conducted routine website reviews to ensure that all websites remain secure. Any websites that are no longer in use are retired to prevent similar attacks from occurring in the future. The SEA also continues to monitor for suspicious network activity. Since the SQL injection attack, similar attacks have been attempted, but were unsuccessful thanks to the agency's work to secure its network.

Lessons Learned

- **Planning helps communications**–The privacy incident response plan enabled agency staff to communicate with each other and coordinate their response to the attack promptly and efficiently.
- **Maintain an inventory**–The SEA has an up-to-date list of all active agency websites to help routinely review website security.

Best Practices and Helpful Resources

✓ **Know your assets**–It is important for agencies to know which websites and applications are in use, particularly those that may be connected to any data, and proactively retire any websites and applications that are no longer used.

✓ **Limit exposure**–The fewer data that are accessible, the less risk that those data can be compromised.

✓ **See something, say something**–Agency staff must know what to do if suspicious activity is observed, including who to report the activity to for further investigation. If suspicious activity isn't reported promptly, it can leave an agency vulnerable to further damage. It is far better to have multiple staff report their concerns than to not have anyone report an incident.

Responding to a Vendor Data Breach

Agency Overview

St. Louis Public Schools, Missouri, has 74 schools with a total student enrollment of approximately 21,800 and a total staff of approximately 2,600.[13] *Note: These numbers represent the most recent ED data and do not necessarily reflect the latest district data.*

Agency's Cybersecurity Approach

St. Louis Public Schools contracted with a vendor for data warehouse and dashboard services. As part of the district's data sharing agreement with vendors, vendors are to notify the district via e-mail, then phone, if a data breach occurs.

Cybersecurity Challenge

In the spring of 2017, the vendor was alerted that it had experienced a data breach via its cloud computing service. The vendor was not aware that the data were publicly exposed until after someone who discovered the data reported the breach on social media.

Agency's Experience

Immediately upon learning of the data breach, St. Louis Public Schools scheduled a conference call with the vendor's president to discuss the incident and the vendor's next steps. The vendor informed the district that the data breach had occurred on a backup server farm and no live data had been exposed. The vendor investigated the incident and confirmed that the backup server location provided an open port that was exploited, but the vendor's production environment was not at risk of a potential hack. Regardless, student information that was included in the backup server's breached dataset should not have been released or shared. The district made it clear that it did not matter whether the data were stored on a backup system or public-facing system since district data were still exposed.

Internally, the district made a notation in all student records within its student information system that outlined the date that the breach occurred. St. Louis Public Schools also posted a notice on its website. Before the incident, the district would upload the latest information from its local system to the vendor's data warehouse system. Following the incident, the district immediately removed some non-pertinent data from its automated uploads, including student address, phone number, parent name, and parent e-mail.

Lessons Learned

- **Prioritize notifications**–The district held the vendors accountable for immediate notification of the data breach and also notified stakeholders of the incident.
- **Limit data availability**–Following the data breach, the district limited the amount of data that are automatically backed up and made available to the vendor.

Best Practices and Helpful Resources

✓ **Review policies and agreements**–Review internal policies and procedures frequently to keep data protected. In addition, make sure that memoranda of understanding (MoUs) and contracts with vendors and external partners protect all data on production servers as well as all backup locations.

13 U.S. Department of Education, National Center for Education Statistics, Common Core of Data (CCD), "Local Education Agency (School District) Universe Survey," 2018-19 v.1a; "Public Elementary/Secondary School Universe Survey," 2018-19 v.1a. Retrieved May 8, 2020, from http://nces.ed.gov/ccd/elsi.

- ✓ **Only share what's necessary**—Consider not providing all requested data to vendors. If there is not a legitimate need to share data with a vendor or external partner, do not provide it.
- ✓ **Don't delay communication**—Establish accountability for vendors to immediately notify clients of any cybersecurity incidents, including data breaches. In turn, immediately notify stakeholders (such as schools, staff, and parents) when an incident occurs.

Recovering from a Ransomware Attack

Agency's Cybersecurity Approach

An unnamed LEA has experienced several challenges in implementing a robust cybersecurity approach. Among the challenges have been cost, awareness, prioritization, staffing, and general impact on resources (time, people, and money), with convenience and affordability often motivating decisions. The district had primarily relied on the expertise of technology department staff to handle cybersecurity matters instead of adopting a comprehensive, agency-wide approach to cybersecurity. There was a misplaced belief that school districts were relatively minor targets (for example, because of a belief that they were too small for cyber-criminals to care about) and a general reliance on "security by obscurity" (meaning a reliance on design or implementation secrecy as the primary security method). Several technical measures—including firewalls, e-mail filtering, internet filtering, and malware software—were in place; however, they were not complemented by non-technical measures, such as enhanced user processes and practices and a dedicated, comprehensive professional development program for all staff. The district's response planning has been insufficient and mandatory user training has not been implemented due to resistance from stakeholders and leadership.

Cybersecurity Challenge

Early in the 2019-20 school year, the LEA experienced a ransomware attack that was initiated by a phishing attack. The district's cybersecurity software blocks multiple phishing attempts every day, but in this case, a phishing message successfully got through to end-users and precipitated the ransomware attack. The incident impacted all schools, departments, and users within the district.

Agency's Experience

Early on a Saturday morning, a district analyst noticed that the LEA's systems were not functioning properly and informed the rest of the technology department about the incident. Even though it was early on a weekend morning, staff reacted quickly to identify the issue and bring systems down. However, the damage had already been done; dozens of systems were rendered unusable.

Technology staff worked over several weeks to restore technology operations across the district. The staff recovered data where possible, rebuilt servers and systems from the ground up, reinstalled most software, and moved some local services to the cloud. Unfortunately, some data were unrecoverable from affected systems. In other cases, data were lost while the data systems were offline (for example, bus ridership data and lunchroom data). The attack only impacted one type of operating system that is used on approximately 15 percent of district computers and most operational servers. So, while most end-user computers were still operational, many of the systems they would typically access were not accessible. District computers running the targeted operating system were unavailable, in some cases for weeks, while they were being rebuilt and systems were restored. In addition, other agency projects were delayed or canceled, and staff lost evenings, vacations, holidays, and weekends to work on the recovery.

The LEA reported the incident to the SEA, local law enforcement, the state cybersecurity office, the Department of Homeland Security, and the FBI. While these agencies were sympathetic, had advice related to responding to the attack, provided recommendations for how to avoid

attacks in the future, and pointed district staff to useful resources, they did not supply any recovery assistance. On the other hand, LEAs from within the state and from other states were particularly helpful in offering assistance, temporarily providing staff, and sharing information based on their own experiences with cybersecurity incidents.

Despite the severity of the incident and the cost (financially and in staff time) to the district, funding, staffing, and user awareness remain a challenge in the wake of the incident. Changes made since the attack have been fairly minimal in scope and primarily isolated to the technology department, rather than being adopted agency-wide. The technology department clearly recognizes the importance of cybersecurity and the need to strengthen its cybersecurity preparedness. The LEA has solicited the help of external experts and resources to assist and critique the district's current measures, with the goal of persuading leadership to adopt a stronger cybersecurity posture moving forward.

Lessons Learned

- **Hindsight helps**–The incident was humbling for the technology department and helped them recognize the cybersecurity risks that LEAs face. It has underscored the need for improved response planning, more thorough documentation, additional resources, and an honest, "warts-and-all" self-evaluation of processes and procedures.
- **Work with others**–The district had been collaborative with peers in the past and reaped some of the benefits of not working in isolation. Following the attack, other LEAs were very helpful in sharing resources and knowledge based on their own experiences. The district has also solicited the help of external experts to help improve its cybersecurity preparedness.
- **Evaluation is necessary**–The incident has motivated the district to engage in critical self-evaluation and third-party assessments.
- **Stay current**–There is a need for professional development for technical and non-technical staff, patches, best practices, and other measures to help the agency and its staff keep up with cybersecurity threats and vulnerabilities.

Best Practices and Helpful Resources

- ✓ **Prioritize security**–User convenience cannot negate robust cybersecurity measures. To be successful, agency leadership and staff need to support an agency-wide approach to cybersecurity.
- ✓ **The human factor**–Technology alone cannot neutralize cybersecurity risks. Requiring cybersecurity training with measurable assessments that must be passed for access to services can reduce risks and vulnerabilities caused by human error.
- ✓ **Use multiple measures**–Technology-based security solutions, like multi-factor authentication, must be complemented by technical and non-technical measures.
- ✓ **Recognize risk**–Third-party cybersecurity experts can help critically assess agency weaknesses, develop strategies to strengthen cybersecurity, and explain to key decisionmakers why cybersecurity must be prioritized.

Conclusion: Best Practices and Lessons Learned

This chapter presented five case studies that detail the actual experiences of SEAs and LEAs that have planned for or experienced a cybersecurity incident. A summary of the best practices and lessons learned from these SEAs and LEAs concludes this chapter, with the goal of helping agencies enhance their cybersecurity practices.

- Agencies need to recognize that they are vulnerable to cybersecurity threats and risks.
- Stakeholders need to support an agency-wide approach to cybersecurity.
- Prioritizing the protection of information and data can help agencies address cyber and data security.
- A robust cybersecurity approach is not contingent on the expertise or capacity of agency staff.

Cybersecurity Training

- Professional development for technical and non-technical staff is necessary for preventing cybersecurity incidents.
- Required training can reduce risks and vulnerabilities caused by human error.
- Best practice materials, such as tip sheets, can help remind agency personnel about cybersecurity.

Cybersecurity Practices

- Agencies need to be proactive and update security practices to protect systems and data from current and new threats.
- Aligning cybersecurity practices within an agency can strengthen agency efforts and impact.
- There are many high-impact, low-cost cybersecurity solutions that agencies can implement with minimal resources.
- Technology solutions must be complemented by technical and non-technical measures.
- User convenience cannot negate robust cybersecurity measures.
- An inventory of agency information and data assets is a helpful tool for routine cybersecurity reviews and updates.
- Peer agencies and external experts can help agencies improve cybersecurity preparedness and respond to an incident.

Cybersecurity Policies

- Limiting access to agency systems, information, and data can minimize the likelihood of an incident.
- Only provide access to a system and its data when there is a legitimate need.
- Frequently review policies and procedures to ensure systems, information, and data are protected.

Cybersecurity Incident Response Planning

- Stakeholder engagement can provide insight into stakeholders' experiences and help agencies design cybersecurity programs that will meet stakeholder needs and solve challenges.
- A cybersecurity incident response plan enables agencies to communicate and coordinate a response promptly and efficiently.
- Response plan tasks should be assigned to specific parties who will be responsible for the task's completion.

- A timely response is critical to containing a cybersecurity incident.
- Promptly reporting suspicious activity can minimize the potential damage of an incident.
- Agency staff must know how to report suspicious activity for further investigation.
- Communication with all relevant stakeholders, such as staff, vendors, and parents, should not be delayed.
- Establish accountability for vendors to immediately notify agencies of any incidents.
- Experiencing an incident can underscore the need for cybersecurity improvements.
- Fully documenting an incident and response, self-evaluation, and third-party assessments can help agencies improve future response efforts.

Appendix A: Cybersecurity Checklist

There are many operational tasks necessary to effectively plan for and respond to a cybersecurity incident. The following list of activities can assist state and local education agencies (SEAs and LEAs) as they create a new cybersecurity response plan or improve an existing one. Additional details about these planning and response activities can be found in chapters 2 through 4. The tasks are not listed in linear order or order of importance; rather, they are best practices that may occur concurrently or in sequential order. This list is not exhaustive or prescriptive, and agencies should modify the tasks and activities in this checklist to best meet their needs. Readers are encouraged to print this checklist and share it with their colleagues.

Actions to Perform Before a Cybersecurity Incident

- ✓ Develop a comprehensive inventory of all network-connected assets.
- ✓ Implement high-impact, low-cost solutions to secure networks, devices, accounts, and passwords.
- ✓ Provide regular training for all end-users of network-connected systems, including students.
- ✓ Secure agency networks, properly configure and segment agency networks, and establish a secure network perimeter.
- ✓ Conduct regular security, systems, and data assessments in a coordinated fashion with stakeholder participation.
- ✓ Consider hiring a third-party expert or Certified Ethical Hacker to assess agency security.
- ✓ Use assessment results to determine whether any systems need to be updated or replaced, and whether any data need to be migrated or destroyed.
- ✓ Enable automated tools and software to identify potential vulnerabilities and protect against threats.
- ✓ Establish a cybersecurity response plan that will be followed when an incident occurs.
- ✓ Align cybersecurity planning activities with related planning and preparation activities.
- ✓ Form a cybersecurity response team and include members from across the agency.
- ✓ Ensure agency leadership understands and supports the response plan.
- ✓ Coordinate with relevant agencies, community partners, vendors, and utility providers, when appropriate.
- ✓ Proactively review federal, state, and local policies and procedures.
- ✓ Adopt comprehensive security plans, protocols, and procedures.

- ✓ Regularly review which data should be collected and which should not.
- ✓ Set criteria for who may, and may not, have access to systems and data.
- ✓ Assign responsibility for monitoring system permissions, regularly monitor who has access, and revoke access when necessary.
- ✓ Examine data retention policies to ensure that data are properly retained and destroyed.
- ✓ Review current insurance policies and coverage for cybersecurity incident protection.
- ✓ Create coherent policies for identity management and passwords.
- ✓ Follow the principle of least privilege.
- ✓ Incorporate cybersecurity into procurement and purchasing processes.
- ✓ Consider the purchase of a retainer for expert forensics services.
- ✓ Review vendor contracts for cybersecurity requirements and responsibilities.

Actions to Perform During a Cybersecurity Incident

- ✓ Report the suspected cybersecurity incident to the specific department/staff responsible for confirming whether an incident has occurred.
- ✓ Confirm that an incident has occurred by examining the available evidence and information.
- ✓ Determine the scope and severity of the incident to identify the impact.
- ✓ Consult the response plan to determine how to proceed.
- ✓ Prioritize essential business functions to help focus response efforts.
- ✓ Consider using alternate or temporary communication methods if regular communication channels are impacted.
- ✓ Contact the agency's cybersecurity insurance provider to ensure that response activities are per policy requirements.
- ✓ Consult legal personnel to determine the agency's responsibilities and requirements, including situations where personally identifiable information (PII) has been exposed.
- ✓ Communicate the response plan to staff at all levels of the agency.
- ✓ Communicate the incident to law enforcement if criminal activity is suspected.
- ✓ Communicate facts about the incident to external stakeholders, including parents.
- ✓ Inventory all systems, determine which systems have been affected, and assess whether any data or information have been compromised.
- ✓ Prepare an alternate data collection process for any collections that must continue while systems are offline/inaccessible.
- ✓ Retrieve any lost data from an alternative source.

Actions to Perform After a Cybersecurity Incident

- ✓ Consult legal counsel's advice on how to proceed with an investigation.
- ✓ Coordinate with law enforcement if criminal activity is suspected.
- ✓ Consider all available options for replacing, upgrading, restoring, and retiring any assets (such as systems, hardware, devices, or software) affected by the incident.
- ✓ Assess the purpose and function of the affected asset, the potential costs and benefits of restoration or replacement, and the security needs of the agency moving forward.
- ✓ Build stronger cybersecurity protections into any systems that are restored or replaced.
- ✓ Use a temporary application, system, or another alternative if necessary.
- ✓ Archive or destroy any temporary systems once they are no longer needed.

- ✓ Consider retaining staff support when recovering from a major incident.
- ✓ Identify funding sources to pay for recovery activities.
- ✓ Prioritize restoring an agency's business operations and mission-critical functions.
- ✓ Retrieve any lost data and records from an alternative source.
- ✓ Key in any data that were collected using temporary paper records.
- ✓ Audit any data that were submitted during the incident.
- ✓ Evaluate the adequacy and effectiveness of the cybersecurity response plan.
- ✓ Solicit feedback from staff to determine the effectiveness of the plan.
- ✓ Use the evaluation results as a catalyst for improved cybersecurity measures.
- ✓ Review and revise business continuity plans, agency processes, and any affected systems based on the evaluation results.
- ✓ Update professional development and training to incorporate preventative measures, response plan updates, and lessons learned.

Appendix B: Resources on Cybersecurity in Education Agencies

The following is a sample list of resources developed by the federal government and state education agencies (SEAs) related to cybersecurity, including data security, in education agencies. This list is not intended to be comprehensive.

Federal Resources

Accessing SLDS Data: Innovative Solutions to State-Specific Security Controls

U.S. Department of Education, Institute of Education Sciences, National Center for Education Statistics, Statewide Longitudinal Data Systems (SLDS) Grant Program

https://slds.ed.gov/#communities/pdc/documents/18796

This spotlight highlights two states, California and Louisiana, with laws that strongly regulate data access. It describes how their state education agencies have adapted their data management and data use procedures to comply with state requirements while continuing to meet their reporting and operational needs.

Best Practices for the Design and Implementation of Data Privacy and Security Programs

U.S. Department of Education, Institute of Education Sciences, National Center for Education Statistics, SLDS Grant Program

https://slds.ed.gov/#communities/pdc/documents/18793

This brief offers an overview of key concepts and content to be covered in privacy and security plans for state SLDS agencies as well as methods of developing and implementing these plans. It draws on best practices identified by the Privacy Technical Assistance Center (PTAC) and includes examples of privacy and security plans from Wisconsin and Kentucky.

Cyber Actors Take Advantage of COVID-19 Pandemic to Exploit Increased Use of Virtual Environments

U.S. Department of Justice, Federal Bureau of Investigation, Internet Crime Complaint Center

https://www.ic3.gov/media/2020/200401.aspx

This public service announcement identifies cybersecurity threats that have increased as a result of the coronavirus disease (COVID-19) pandemic and provides recommendations to counteract these threats.

Cyber Investigations

U.S. Department of Homeland Security, U.S. Secret Service

https://www.secretservice.gov/investigation/#cyber

The U.S. Secret Service cybercrime mission has expanded the scope of its investigative efforts beyond its traditional limits. As part of its mandate to combat financially motivated cybercrime, the U.S. Secret Service complements its investigative efforts with educational outreach programs. These programs are aimed at strengthening the ability of private and public sector entities to protect themselves against an array of cybercrime.

Cybersecurity and Remote Learning and Working

U.S. Department of Education, Institute of Education Sciences, National Center for Education Statistics, National Forum on Education Statistics and SLDS Grant Program

https://slds.grads360.org/#communities/pdc/documents/18939

The Forum and the SLDS Grant Program joined efforts for Steven Hernandez, chief information security officer for the U.S. Department of Education, to deliver a virtual presentation. The webinar provided information on the security implications of virtual education technologies and shared best practices for securing agency information and data while working and learning remotely.

Cybersecurity Considerations for K-12 Schools and School Districts

U.S. Department of Education, Office of Safe and Supportive Schools, Readiness and Emergency Management for Schools Technical Assistance Center

https://rems.ed.gov/docs/Cybersecurity_K-12_Fact_Sheet_508C.PDF

This fact sheet focuses on addressing threats to a school's or school district's networks and systems, also called cybersecurity considerations.

Data Breach Response Checklist

U.S. Department of Education, Student Privacy Policy Office

https://studentprivacy.ed.gov/resources/data-breach-response-checklist

This checklist of critical breach response components and steps is intended to assist education agencies in building a comprehensive data breach response capability. It is meant to be used as a general example illustrating current industry best practices in data breach response and mitigation applicable to the education community.

Data Security and Management Training: Best Practice Considerations

U.S. Department of Education, Student Privacy Policy Office

https://studentprivacy.ed.gov/resources/data-security-and-management-training-best-practice-considerations

This brief provides best practices for data security and data management training for education leaders. It discusses key training concepts to follow, content, delivery methods, and possible audiences for training.

Data Security Checklist

U.S. Department of Education, Student Privacy Policy Office

https://studentprivacy.ed.gov/resources/data-security-checklist

This checklist is designed to assist education agencies with developing and maintaining a successful data security program by listing essential components that should be considered when building such a program, with a focus on solutions and procedures relevant for supporting data security operations of education agencies.

Data Security Threats: Education Systems in the Crosshairs

U.S. Department of Education, Student Privacy Policy Office

https://studentprivacy.ed.gov/resources/data-security-threats-education-systems-crosshairs

This presentation reviews security threats to education data systems, including common ways in which these systems can be exploited. It also offers suggestions on assessing system vulnerabilities and mitigating the risks.

Family Educational Rights and Privacy Act (FERPA) and the Coronavirus Disease 2019 (COVID-19)

U.S. Department of Education, Student Privacy Policy Office

https://studentprivacy.ed.gov/resources/ferpa-and-coronavirus-disease-2019-covid-19

The purpose of this guidance is to answer questions that school officials may have had concerning the disclosure of personally identifiable information from students' education records to outside entities during the coronavirus disease (COVID-19) pandemic.

FERPA and Virtual Learning During COVID-19

U.S. Department of Education, Student Privacy Policy Office

https://studentprivacy.ed.gov/training/ferpa-and-virtual-learning-during-covid-19-webinar-recording

This webinar is intended to provide information on privacy best practices and insight into helpful resources available to the education community during the coronavirus disease (COVID-19) pandemic.

Federal Risk and Authorization Management Program (FedRAMP)

General Services Administration

https://www.fedramp.gov/

FedRAMP is a cybersecurity risk management program by which the U.S. federal government determines whether cloud products and services are secure enough for purchase and use by federal agencies. The FedRAMP Marketplace provides a database of cloud services that have achieved a FedRAMP designation.

How to Engage and Train Stakeholders Regarding Privacy and Security Best Practices

U.S. Department of Education, Institute of Education Sciences, National Center for Education Statistics, SLDS Grant Program

https://slds.ed.gov/#communities/pdc/documents/18506

This brief offers an overview of key concepts and content to be covered in privacy and security training for SEAs as well as methods of delivering that content to stakeholders. It draws on best

practices identified by PTAC and includes examples of privacy and security training among state agencies involved in Utah's SLDS.

Integrating Cybersecurity with Emergency Operations Plans (EOPs) for K-12 Schools

U.S. Department of Education, Office of Safe and Supportive Schools, Readiness and Emergency Management for Schools Technical Assistance Center

https://rems.ed.gov/IntegratingCybersecurityForK12.aspx

In this webinar, presenters provided an overview of the landscape of cybersecurity threats facing K-12 schools. Resources, programs, and tools to help schools maintain secure networks and prevent cyber-attacks were also shared.

Issue Brief: Data Security Top Threats to Data Protection

U.S. Department of Education, Student Privacy Policy Office

https://studentprivacy.ed.gov/resources/issue-brief-data-security-top-threats-data-protection

This brief outlines critical technical and non-technical threats to education data and information systems. A brief description of each threat is followed by a suggestion of appropriate risk mitigation measures.

Keeping Children Safe Online

U.S. Department of Justice

https://www.justice.gov/coronavirus/keeping-children-safe-online

This webpage provides guidance for teachers, parents, guardians, and caregivers on protecting children from becoming victims of online child predators during school closures due to the coronavirus disease (COVID-19) pandemic.

National Cybersecurity Assessments and Technical Services (NCATS)

U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency

https://www.us-cert.gov/resources/ncats

The NCATS team supports federal, state, and local governments and critical infrastructure partners by providing proactive testing and assessment services. NCATS provides its stakeholders with an objective third-party perspective of their operational cybersecurity posture, identifies security control strengths and weaknesses, and actionable reports that champion the implementation of mitigations and controls capable of positive impact toward reduction of overall risk.

National Infrastructure Protection Plan (NIPP) Government Facilities Sector-Specific Plan for 2015

U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency

https://www.cisa.gov/publication/nipp-ssp-government-facilities-2015

The Government Facilities Sector-Specific Plan details how the NIPP risk management framework is implemented within the context of the unique characteristics and risk landscape of the sector. Each Sector-Specific Agency develops a sector-specific plan through a coordinated effort involving its public and private sector partners. The Education Facilities Subsector includes facilities that are owned by both government and private sector entities and covers pre-kindergarten through 12th-grade schools, institutions of higher education, and business and trade schools.

NIST Special Publication (SP) 800-53

U.S. Department of Commerce, National Institute of Standards and Technology (NIST)

https://nvd.nist.gov/800-53

The NIST SP 800-53 database represents the security controls and associated assessment procedures defined in NIST SP 800-53 (Revision 4) Security Controls for Federal Information Systems and Organizations.

Responding to Information Technology (IT) Security Audits: Improving Data Security Practices

U.S. Department of Education, Student Privacy Policy Office

https://studentprivacy.ed.gov/resources/responding-it-security-audits-improving-data-security-practices

IT audits can help organizations identify critical gaps in data security and reduce the threat of security compromises. This issue brief explains what audits are and how they can be used to improve data security.

Secure Video Conferencing for Schools

U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency

https://www.cisa.gov/publication/secure-video-conferencing-schools

These resources provide cybersecurity recommendations and guidance for K-12 schools to help keep schools, staff, and students safe while videoconferencing.

SITE ASSESS: A Mobile Application (App) for K-12 Schools, School Districts, and Institutions of Higher Education

U.S. Department of Education, Office of Safe and Supportive Schools, Readiness and Emergency Management for Schools Technical Assistance Center

https://rems.ed.gov/SITEASSESS.aspx

This free, secure, and comprehensive mobile app is designed for school district and school personnel to examine their security, safety, accessibility, and emergency preparedness. The app generates a customized to-do list that may be used in the short term and long term to address facility improvements, prompts teams to share pertinent information with first responders, and contains relevant resources on education facility and preparedness topics. Included within the section on Computers and Network Systems are tasks that examine cybersecurity.

SP 1800-series Documents

U.S. Department of Commerce, National Institute of Standards and Technology (NIST)

https://csrc.nist.gov/publications/sp1800

NIST SP 1800-series documents present practical, usable, cybersecurity solutions to demonstrate how to apply standards-based approaches and best practices. Each publication generally serves as a "how-to" guide that is designed to help organizations gain efficiencies in implementing cybersecurity technologies while saving them research and proof of concept costs.

Cybersecurity

Colorado Department of Public Safety

https://www.colorado.gov/pacific/cssrc/cyber-security

This webpage provides information and links to helpful resources on cybersecurity in local education agencies (LEAs) and schools.

Cybersecurity

Indiana Department of Education

https://www.doe.in.gov/cybersecurity

This initiative funded several activities to improve the cybersecurity position of Indiana schools, including a cybersecurity training and awareness service for K-12 school personnel, funding for high school cybersecurity coursework, and matching grants for schools to improve their e-security stance. The following webpages include additional information related to the initiative:

- Cybersecurity Task Force Cyber Blog (https://www.indianactocouncil.org/domain/39).
- Resource Hub (https://www.doe.in.gov/cybersecurity/resource-hub).
- Indiana K-12 Cybersecurity Audit Checklist (https://docs.google.com/spreadsheets/d/11vdbs4_Eh8RohaOPH_V0ksmT37JzxsE4K_UWyc5WTaM/edit?usp=sharing).

Cybersecurity Task Force

California Office of Emergency Services

https://www.caloes.ca.gov/cal-oes-divisions/cybersecurity-task-force

This webpage provides information on the California Cybersecurity Task Force, a statewide partnership comprised of key stakeholders, experts, and professionals from California's public, private, academic, and law enforcement sectors.

Data Privacy

California Department of Education

https://www.cde.ca.gov/ds/ed/dataprivacy.asp

This webpage provides information and links to laws, policies, and best practices on data privacy for parents, teachers, local education agencies, and the general public.

Data Privacy and Security

Colorado Department of Education

https://www.cde.state.co.us/dataprivacyandsecurity

These webpages contain federal and state policies that the Colorado Department of Education adheres to, data privacy and security procedures, as well as guidance and resources for various stakeholders.

Data Privacy and Security

Kentucky Department of Education

https://education.ky.gov/districts/tech/Pages/Data-Security-Privacy.aspx

The webpage serves as a hub for information on data privacy and security. It includes links to applicable federal and state laws, policies, and best practices established by the Kentucky Department of Education, and resources and training by audience and topic.

IT Security Incident Communication

Washington State Office of the Chief Information Officer

https://ocio.wa.gov/policy/it-security-incident-communication

This policy was created to ensure the scope and impact of IT security incidents are properly evaluated, and that a coordinated, centralized approach is used to determine if, when, and how to communicate notification of an incident.

North Dakota Computer Science and Cybersecurity K-12 Standards

North Dakota Department of Public Instruction

https://www.nd.gov/dpi/sites/www/files/documents/Academic%20Support/CSCS2019.pdf

These learning standards provide North Dakota educators, school administrators, and parents the information they need about what students should know and be able to do about computer science and cybersecurity from kindergarten through high school. The standards set expectations for student learning to increase student awareness of the importance of cybersecurity in schools and the workplace.

Privacy of Pupil Records

California Education Code

https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=EDC&sectionNum=49073.1

This state legislation sets requirements for California LEAs to protect the privacy of student records, including situations in which an LEAs contracts with a third party to provide software or services for the digital storage, management, and retrieval of student records.

Reference List

Citations

American Council for Technology and Industry Advisory Council. (n.d.). *Zero Trust Cybersecurity*. Retrieved July 27, 2020, from https://www.actiac.org/hot-topics/zero-trust-cybersecurity.

Children's Internet Protection Act, P.L. 106-554 114 Stat. 2763 (2000)

Children's Online Privacy Protection Act of 1998, 15 U.S.C. § 6501-6506 (1998)

Daviess County Public Schools. (n.d.). *DCPS Digital Citizenship*. Retrieved April 23, 2020, from https://sites.google.com/daviess.kyschools.us/dcpsdigcit/home.

Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g (1974)

Health Insurance Portability and Accountability Act of 1996, P.L. 104-191 110 Stat. 1936 (1996)

Levin, D. A., "K-12 Cyber Incident Map," 2016-19. Retrieved December 31, 2019, from https://k12cybersecure.com/map/.

Levin, D. A., "K-12 Cyber Incidents," 2019. Retrieved March 9, 2020, from https://k12cybersecure.com/blog/state-of-k-12-cybersecurity-2019-year-in-review/2019-incidents.

Levin, D. A. (2020). *The State of K-12 Cybersecurity: 2019 Year in Review*. Retrieved March 9, 2020, from https://k12cybersecure.com/year-in-review/.

National Conference of State Legislatures. (2017). *State Cybersecurity Training for State Employees*. Retrieved June 22, 2020, from https://www.ncsl.org/ncsl-in-dc/standing-committees/law-criminal-justice-and-public-safety/state-cybersecurity-training-for-state-employees.aspx.

National Forum on Education Statistics. (2016). *Forum Guide to Education Data Privacy* (NFES 2016-096). U.S. Department of Education. Washington, DC: National Center for Education Statistics. Retrieved December 27, 2019, from https://nces.ed.gov/forum/pub_2016096.asp.

National Forum on Education Statistics. (2019). *Forum Guide to Technology Management in Education* (NFES 2019161). U.S. Department of Education. Washington, DC: National Center for Education Statistics. Retrieved December 26, 2019, from https://nces.ed.gov/forum/tec_intro.asp.

National Forum on Education Statistics. (2019). *Forum Guide to Planning for, Collecting, and Managing Data About Students Displaced by a Crisis* (NFES 2019-163). U.S. Department of Education. Washington, DC: National Center for Education Statistics. Retrieved December 27, 2019, from https://nces.ed.gov/forum/pub_2019163.asp.

National Forum on Education Statistics. (2020). *Forum Guide to Data Governance* (NFES 2020-083). U.S. Department of Education. Washington, DC: National Center for Education Statistics. Retrieved July 27, 2020, from https://nces.ed.gov/forum/pub_2020083.asp.

Sheridan, K. (2019, September 20). *Ransomware Strikes 49 School Districts & Colleges in 2019*. Retrieved March 9, 2020, from https://www.darkreading.com/threat-intelligence/ransomware-strikes-49-school-districts-and-colleges-in-2019/d/d-id/1335872.

Student Data Privacy Consortium. (n.d.). *SDPC Resource Registry*. Retrieved April 24, 2020, from https://sdpc.a4l.org/search_national.php.

U.S. Department of Commerce, National Institute of Standards and Technology. (2010). *Contingency Planning Guide for Federal Information Systems*. Retrieved December 23, 2019, from https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf.

U.S. Department of Commerce, National Institute of Standards and Technology. (2012). *Cloud Computing Synopsis and Recommendations*. Retrieved April 24, 2020, from https://doi.org/10.6028/NIST.SP.800-146.

U.S. Department of Commerce, National Institute of Standards and Technology. (2017). *An Introduction to Information Security*. Retrieved January 8, 2020, from https://doi.org/10.6028/NIST.SP.800-12r1.

U.S. Department of Commerce, National Institute of Standards and Technology. (2020). *Zero Trust Architecture*. Retrieved August 26, 2020, from https://csrc.nist.gov/publications/detail/sp/800-207/final.

U.S. Department of Commerce, National Institute of Standards and Technology. (n.d.). *NIST Special Publication 800-53*. Retrieved July 27, 2020, from https://nvd.nist.gov/800-53.

U.S. Department of Education, National Center for Education Statistics, Common Core of Data (CCD), "Local Education Agency (School District) Universe Survey," 2018-19 v.1a; "Public Elementary/Secondary School Universe Survey," 2018-19 v.1a. Retrieved May 8, 2020, from http://nces.ed.gov/ccd/elsi.

U.S. Departments of Education and Health and Human Services. (2019). *Joint Guidance on the Application of the Family Educational Rights and Privacy Act (FERPA) and the Health Insurance Portability and Accountability Act of 1996 (HIPAA) to Student Health Records*. Retrieved April 23, 2020, from https://studentprivacy.ed.gov/resources/joint-guidance-application-ferpa-and-hipaa-student-health-records.

U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency and U.K. National Cyber Security Centre. (2020). *Alert (AA20-099A) COVID-19 Exploited by Malicious Cyber Actors*. Retrieved April 29, 2020, from https://www.us-cert.gov/ncas/alerts/aa20-099a.

U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency. (n.d.). *National Cybersecurity Assessments and Technical Services*. Retrieved April 29, 2020, from https://www.us-cert.gov/resources/ncats.

U.S. Department of Homeland Security, U.S. Secret Service. (n.d.). *Cyber Investigations*. Retrieved July 27, 2020, from https://www.secretservice.gov/investigation/#cyber.

U.S. Department of Justice, Computer Crime and Intellectual Property Section. (2018). *Reporting Computer, Internet-related, Or Intellectual Property Crime*. Retrieved December 23, 2019, from https://www.justice.gov/criminal-ccips/reporting-computer-internet-related-or-intellectual-property-crime.

Additional Resources

California IT in Education. (n.d.). *California Student Privacy Alliance*. Retrieved March 3, 2020, from https://cite.org/page/StuPrivacy/.

Castelo, M. (2020, April 15). *4 Cyberhygiene Practices for Secure Remote Learning*. EdTech: Focus on K-12. Retrieved June 19, 2020, from https://edtechmagazine.com/k12/article/2020/04/4-cyberhygiene-practices-secure-remote-learning.

Center for Internet Security. (2020). *Multi-State Information Sharing & Analysis Center.* Retrieved April 29, 2020, from https://www.cisecurity.org/ms-isac/.

Connolly, J., & Arensdorff, M. (2019, April). *Cyber & Physical Security - Practical Tips from Two Illinois K-8 and 9-12 Districts*. Presented at the annual meeting of the Consortium for School Networking, Portland. Retrieved May 6, 2019, from https://tinyurl.com/y79bm5gr.

Consortium for School Networking. (2017). *District Security Checklist*. Retrieved May 6, 2019, from https://www.cosn.org/sites/default/files/2017%20Cybersecurity%20checklist.pdf.

Consortium for School Networking. (2017). *Getting Started with Cybersecurity.* Retrieved June 17, 2019, from https://www.cosn.org/sites/default/files/Getting%20Started%20with%20Cybersecurity_ALV_Oct2017_PRINTversion.pdf.

Consortium for School Networking. (2017). *Security Planning Rubric*. Retrieved May 6, 2019, from http://cosn.org/sites/default/files/2017%20Cybersecurity%20rubric.pdf.

Consortium for School Networking. (2018). *Cybersecurity*. Retrieved May 6, 2019, from http://cosn.org/cybersecurity.

Consortium for School Networking. (2018). *Cybersecurity: Protecting Student Cyber AND Physical Security*. Retrieved December 14, 2018, from http://cosn.org/events/webinars/cybersecurity-protecting-student-cyber-and-physical-security.

Consortium for School Networking. (2018). *What Are Cyber-Physical Security Systems?* Retrieved May 6, 2019, from https://www.cosn.org/sites/default/files/Cyber%20and%20Physical%20Security%20Systems.pdf.

Consortium for School Networking. (2020). *Cybersecurity Considerations in a COVID-19 World*. Retrieved June 19, 2020, from https://covid19edtechguidance.com/cybersecurity-considerations-in-a-covid-19-world/.

Federal Communications Commission, Consumer and Governmental Affairs Bureau. (2019). *Children's Internet Protection Act (CIPA)*. Retrieved October 8, 2020, from www.fcc.gov/file/15349/download.

Indiana Chief Technology Officer (CTO) Council. (2020). *Indiana CTO Council*. Retrieved February 26, 2020, from https://www.indianactocouncil.org/.

National Cyber Security Alliance. (n.d.). *Stop. Think. Connect*. Resources. Retrieved March 3, 2020, from https://www.stopthinkconnect.org/resources.

National Forum on Education Statistics and Statewide Longitudinal Data Systems Grant Program. (2020, April). *Cybersecurity and Remote Learning and Working*. Retrieved April 29, 2020, from https://slds.grads360.org/#communities/pdc/documents/18939.

Ritchey, D. (2018, April 1). *The Unstoppable Convergence Between Physical and Cybersecurity*. Security Magazine. Retrieved June 17, 2019, from https://www.securitymagazine.com/articles/88847-the-unstoppable-convergence-between-physical-and-cybersecurity.

U.S. Department of Commerce, National Institute of Standards and Technology, Computer Security Resource Center. (n.d.). *Glossary*. Retrieved January 8, 2020, from https://csrc.nist.gov/glossary.

U.S. Department of Defense, National Security Agency. (2018). *Top Ten Cybersecurity Mitigation Strategies*. Retrieved from https://apps.nsa.gov/iaarchive/library/ia-guidance/security-tips/nsas-top-ten-cybersecurity-mitigation-strategies.cfm.

U.S. Department of Education, Office of Safe and Supportive Schools, Readiness and Emergency Management for Schools Technical Assistance Center. (2017). *Cybersecurity Considerations for K-12 Schools and School Districts*. Retrieved November 27, 2019, from https://rems.ed.gov/docs/Cybersecurity_K-12_Fact_Sheet_508C.PDF.

U.S. Department of Education, Student Privacy Policy Office. (n.d.). *Glossary*. Retrieved December 11, 2019, from https://studentprivacy.ed.gov/glossary.

U.S. Department of Education, Student Privacy Policy Office. (2012). *Data Breach Response Checklist*. Retrieved July 30, 2019, from https://studentprivacy.ed.gov/resources/data-breach-response-checklist.

U.S. Department of Education, Student Privacy Policy Office. (2015). *Data Security and Management Training: Best Practice Considerations*. Retrieved December 27, 2019, from https://studentprivacy.ed.gov/resources/data-security-and-management-training-best-practice-considerations.

U.S. Department of Education, Student Privacy Policy Office. (2015). *Identity Authentication Best Practices*. Retrieved January 8, 2020, from https://studentprivacy.ed.gov/resources/identity-authentication-best-practices.

U.S. Department of Education, Student Privacy Policy Office. (2015). *Issue Brief: Data Security Top Threats to Data Protection*. Retrieved January 8, 2020, from https://studentprivacy.ed.gov/resources/issue-brief-data-security-top-threats-data-protection.

U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, Computer Emergency Readiness Team. (2013). *Computer Forensics*. Retrieved April 27, 2020, from https://www.us-cert.gov/security-publications/computer-forensics.

U.S. Department of Justice, Computer Crime and Intellectual Property Section, Cybersecurity Unit. (2018). *Best Practices for Victim Response and Reporting of Cyber Incidents, Version 2.0*. Retrieved April 29, 2020, from https://www.justice.gov/criminal-ccips/file/1096971/download.

Related Resources

Relevant National Forum on Education Statistics Resources

Forum Guide to Data Governance (2020)

https://nces.ed.gov/forum/pub_2020083.asp

This resource provides timely and useful best practices, examples, and resources for agencies implementing or updating their data governance programs. It provides an overview of data governance; discusses effective data governance practices, structures, and essential elements; describes how to meet privacy and security requirements while also meeting data accessibility and sharing needs; and includes detailed case studies from education agencies in their data governance efforts.

Forum Guide to Education Data Privacy (2016)

https://nces.ed.gov/forum/pub_2016096.asp

This resource provides SEAs and LEAs with best practice information to use in assisting school staff in protecting the confidentiality of student data in instructional and administrative practices. SEAs and LEAs may also find the guide useful in developing privacy programs and related professional development programs.

Forum Guide to Planning for, Collecting, and Managing Data About Students Displaced by a Crisis (2019)

https://nces.ed.gov/forum/pub_2019163.asp

This resource provides timely and useful best practice information for collecting and managing data about students who have enrolled in another school or district because of a crisis. It highlights best practices that education agencies can adopt before, during, and after a crisis and features contributions from agencies that have either experienced a crisis or received students who were displaced by a crisis.

Forum Guide to Technology Management in Education (2019)

https://nces.ed.gov/forum/tec_intro.asp

This resource is designed to assist education agency staff with understanding and applying best practices for selecting and implementing technology to support teaching and learning in the classroom. It addresses the widespread use and integration of technology in modern education systems and focuses on technology governance and planning, technology implementation, integration, maintenance, support, training, privacy, security, and evaluation.

Other National Forum on Education Statistics Resources

Forum Curriculum for Improving Education Data: A Resource for Local Education Agencies (2007)

https://nces.ed.gov/forum/pub_2007808.asp

This curriculum supports efforts to improve the quality of education data by serving as training materials for K-12 school and district staff. It provides lesson plans, instructional handouts, and related resources, and presents concepts necessary to help schools develop a culture for improving data quality.

Forum Guide to Alternative Measures of Socioeconomic Status in Education Data Systems (2015)

https://nces.ed.gov/forum/pub_2015158.asp

This resource provides "encyclopedia-type" entries for eight plausible alternative measures of socioeconomic status (SES) and, as such, will help readers better understand the implications of collecting and interpreting a range of SES-related data in education agencies.

Forum Guide to Building a Culture of Quality Data: A School & District Resource (2004)

https://nces.ed.gov/forum/pub_2005801.asp

This resource was developed to help schools and school districts improve the quality of data they collect and to provide processes for developing a "Culture of Quality Data" by focusing on data entry—getting things right at the source. This resource shows how quality data can be achieved in a school or district through the collaborative efforts of all staff.

Forum Guide to Collecting and Using Attendance Data (2018)

https://nces.ed.gov/forum/pub_2017007.asp

This resource is designed to help state and local education agency staff (SEA and LEA) improve their attendance data practices. It offers best practice suggestions and real-life examples, a set of voluntary attendance codes, and tip sheets for a wide range of education agency staff who work with attendance data.

Forum Guide to Collecting and Using Disaggregated Data on Racial/Ethnic Subgroups (2016)

https://nces.ed.gov/forum/pub_2017017.asp

This resource is intended to identify some of the overarching benefits and challenges involved in data disaggregation; recommend appropriate practices for disaggregating racial/ethnic data in districts and states; and describe real-world examples of large and small education agencies disaggregating racial/ethnic data successfully.

Forum Guide to College and Career Ready Data (2015)

https://nces.ed.gov/forum/pub_2015157.asp

This resource outlines the data needs and helpful analytics for five use cases (individual learning plans, educator support systems, postsecondary feedback loops, accountability systems, and career technical and education programs) that support SEA and LEA college and career-ready initiatives.

Forum Guide to Core Finance Data Elements (2007)

https://nces.ed.gov/forum/pub_2007801.asp

This resource provides an overview of key finance data terms. It also covers the two National Center for Education Statistics (NCES) public school finance surveys: the state-level National Public Education Financial Survey and the School District Finance Survey (or F-33).

Forum Guide to Crime, Violence, and Discipline Incident Data (2011)

https://nces.ed.gov/forum/pub_2011806.asp

This resource focuses on the use of crime, violence, and discipline data to improve school safety. It presents strategies for implementing an incident database; recommends a body of data elements, definitions, and code lists useful for collecting accurate and comparable data; and offers suggestions for the effective presentation and reporting of data.

Forum Guide to Data Ethics (2010)

http://nces.ed.gov/forum/pub_2010801.asp

While laws set the legal parameters that govern data use, ethics establish fundamental principles of "right and wrong" that are critical to the appropriate management and use of education data in the technology age. This guide reflects the experience and judgment of seasoned data managers; while there is no mandate to follow these principles, it is hoped that the contents will prove a useful reference to others in their work.

Forum Guide to Data Visualization: A Resource for Education Agencies (2016)

https://nces.ed.gov/forum/pub_2017016.asp

This resource recommends data visualization practices that will help education agencies communicate data meaning in visual formats that are accessible, accurate, and actionable for a wide range of education stakeholders. Although this resource is designed for staff in education agencies, many of the visualization principles apply to other fields as well.

Forum Guide to Decision Support Systems: A Resource for Educators (2006)

https://nces.ed.gov/forum/pub_2006807.asp

This resource was developed to remedy the lack of reliable, objective information available to the education community about decision support systems. It is intended to help readers better understand what decision support systems are, how they are configured, how they operate, and how they might be developed and implemented in an education setting.

Forum Guide to Education Indicators (2005)

https://nces.ed.gov/forum/pub_2005802.asp

This resource provides encyclopedia-type entries for 44 commonly used education indicators. Each indicator entry contains a definition, recommended uses, usage caveats and cautions, related policy questions, data element components, a formula, commonly reported subgroups, and display suggestions.

Forum Guide to Elementary/Secondary Virtual Education Data (2016)

https://nces.ed.gov/forum/pub_2016095.asp

This resource provides information on the impact of virtual education on established data elements and methods of data collection and addresses the scope of changes, the rapid pace of new technology development, and the proliferation of resources in virtual education.

Forum Guide to Ensuring Equal Access to Education Websites (2011)

https://nces.ed.gov/forum/pub_2011807.asp

This resource guides education institutions in improving the accessibility of websites and other electronic information technology, and in complying with accessibility standards and laws. It is intended to raise awareness in nontechnical audiences and suggest best practices for complying with Section 508 goals at an operational level in schools, school districts, and SEAs.

Forum Guide to Exit Codes (2020)

https://nces.ed.gov/forum/pub_2020132.asp

This resource provides best practice information for tracking data about when students exit an education agency. It defines exit codes and reviews their use in an education agency; provides a voluntary, common taxonomy for exit codes; discusses best practices and methods for exit

codes data collection; and features case studies that highlight different education agencies' approaches to and experiences with exit coding.

Forum Guide to Facility Information Management: A Resource for State and Local Education Agencies (2018)

https://nces.ed.gov/forum/pub_2018156.asp

This resource is designed to help SEAs and LEAs plan, design, build, use, and improve their facility information systems. It includes a review of why school facilities data matter and recommends a five-step process that an education agency can undertake to develop a robust facility information system around goals, objectives, and indicators.

Forum Guide to Metadata: The Meaning Behind Education Data (2009)

https://nces.ed.gov/forum/pub_2009805.asp

This resource offers best practice concepts, definitions, implementation strategies, and templates/tools for an audience of data, technology, and program staff in SEAs and LEAs. It is hoped that this resource will improve this audience's awareness and understanding of metadata and, subsequently, the quality of the data in the systems they maintain.

Forum Guide to Personalized Learning Data (2019)

https://nces.ed.gov/forum/pub_2019160.asp

This resource will help education agencies as they consider whether and how to expand their use of personalized learning. It includes an overview of the topic, best practices on collecting and using data for personalized learning, and case studies from districts and states that have implemented personalized learning.

Forum Guide to School Courses for the Exchange of Data (SCED) Classification System (2014)

https://nces.ed.gov/forum/pub_2014802.asp

SCED is a voluntary, common classification system for prior-to-secondary and secondary school courses. This resource includes an overview of the SCED structure and descriptions of the SCED Framework elements, recommended attributes, and information for new and existing users on best practices for implementing and expanding their use of SCED.

Forum Guide to Supporting Data Access for Researchers: A Local Education Agency Perspective (2014)

https://nces.ed.gov/forum/pub_2014801.asp

This resource recommends a set of core practices, operations, and templates that can be adopted and adapted by LEAs as they consider how to respond to requests for both new and existing data about the education enterprise.

Forum Guide to Supporting Data Access for Researchers: A State Education Agency Perspective (2012)

https://nces.ed.gov/forum/pub_2012809.asp

This resource recommends a set of core practices, operations, and templates that can be adopted and adapted by SEAs as they consider how to respond to requests for data about the education enterprise, including data maintained in longitudinal data systems.

Forum Guide to Taking Action with Education Data (2013)

https://nces.ed.gov/forum/pub_2013801.asp

This resource provides practical information about the knowledge, skills, and abilities needed to identify, access, interpret, and use data to improve instruction in classrooms and the operation of schools, LEAs, and SEAs.

Forum Guide to the Teacher-Student Data Link: A Technical Implementation Resource (2013)

https://nces.ed.gov/forum/pub_2013802.asp

This resource is intended as a guide to the skillful and appropriate use of education data. It introduces the teacher-student data link (TSDL) and provides information on TSDL components, use cases, and strategies for overcoming implementation challenges.

Managing an Identity Crisis: Forum Guide to Implementing New Federal Race and Ethnicity Categories (2008)

https://nces.ed.gov/forum/pub_2008802.asp

This best-practice resource was developed to assist SEAs and LEAs in their implementation of the new federal race and ethnicity categories—thereby reducing redundant efforts within and across states, improving data comparability, and minimizing reporting burden. It serves as a toolkit from which users may select and adopt strategies that will help them quickly begin the process of implementation in their agencies.

Traveling Through Time: The Forum Guide to Longitudinal Data Systems (Series)

Book I: What is an LDS? (2010) http://nces.ed.gov/forum/pub_2010805.asp

Book II: Planning and Developing an LDS (2011) http://nces.ed.gov/forum/pub_2011804.asp

Book III: Effectively Managing LDS Data (2011) http://nces.ed.gov/forum/pub_2011805.asp

Book IV: Advanced LDS Usage (2011) http://nces.ed.gov/forum/pub_2011802.asp

The *Traveling Through Time* series is intended to help SEAs and LEAs meet the many challenges involved in developing robust systems, populating them with quality data, and using this new information to improve the education system. The series introduces important topics, offers best practices, and directs the reader to additional resources related to longitudinal data system (LDS) planning, development, management, and use.