SLDS Issue Brief

Securing Your SLDS

As the collection and use of education data continue to grow, so do the chances for those data to be lost, inappropriately accessed, or stolen. For many organizations that store data, the question is not whether their data security will be compromised, but when.

Since 2009, there have been six known data breaches in state education agencies. These breaches have cost states more than a half million dollars and risked revealing the personal information of hundreds of thousands of students and teachers. In addition to complying with legal requirements and protecting the privacy of their students, education agencies must shield themselves from the costs and reputational harm caused by a data breach.

This brief describes common threats to the security of education data systems, steps that education agencies should take to minimize the risk of a data breach, and strategies for addressing the effectiveness of data security measures.

Data Security in Education Data Systems

Several characteristics of education data systems place them at risk for security breaches. These data systems often connect to public-facing websites and applications, facilitate large-scale transfers of data between systems, and involve numerous user accounts and remote data collections. Data systems that span multiple agencies—such as P-20W+ (early childhood through workforce) SLDSs—must also manage interagency data connections and differences in how data are handled and stored by the various partners.

Legal requirements for data security

Although the federal Family Educational Rights and Privacy Act (FERPA) requires education agencies to implement "reasonable methods" to prevent the unauthorized disclosure of students' private information, the law does not detail specific security measures. The U.S. Department of Education's Privacy Technical Assistance Center (PTAC) recommends that education agencies implement a set of security controls that are in line with current accepted practices for data of a similar sensitivity.

States may place additional requirements on education agencies to protect data. Agencies must ensure that security protocols include measures imposed by state law as well as industry best practices.

Understanding the risks to education data

Security risks to education data represent a combination of threats to the privacy and security of data and a data system's vulnerability to those threats.

A **data breach** is any instance of unauthorized access or release of personally identifiable information (PII) or other information not suitable for public release. Common types of data breaches include malicious attacks by hackers; lost, stolen, or misplaced equipment; and failure of security policies or systems.

This product of the Institute of Education Sciences (IES) SLDS Grant Program was developed with the help of knowledgeable staff from state education agencies and partner organizations. The content was derived from a regional workshop facilitated by the Privacy Technical Assistance Center in August 2017. The information presented does not necessarily represent the opinions of the IES SLDS Grant Program. We thank the following people for their valuable contributions:

Ross Lemke
Mike Tassey
Privacy Technical Assistance Center

Baron Rodriguez
SLDS Grant Program, State Support Team

For more information on the IES SLDS Grant Program or for support with system development, please visit http://nces.ed.gov/programs/SLDS.

Security threats
Threats to data security can come from both inside and outside the education agency. Internal threats might include the following:

- *Mistakes*. Agency employees might inadvertently expose data to unauthorized use through errors or lapses in judgment. Mistakes can include falling for “phishing” email scams, misaddressing emails or other communications containing sensitive data, or losing or improperly securing equipment that could then be stolen.
- *Intentional misconduct*. Employees could disclose sensitive data on purpose, possibly for personal gain.
- *Curiosity*. Employees’ interest in information or processes might lead them to access data improperly or allow others to access data.
- *Poor practices*. Behaviors such as unsafe internet browsing habits, using unsecured wireless internet connections, sending email attachments that contain personally identifiable information, and using weak passwords to protect data can put sensitive data at risk.

External threats to data security might include the following:

- *Hackers and cyber-criminals*. Individuals outside the education agency can attempt to break into secure systems, usually for financial gain. Criminals might try to target education agencies to steal employees’ identities or Form W-2 information or to commit financial crimes.
- *Social engineering attacks*. Email-based scams such as “phishing” attacks might be used to gain sensitive information from employees by impersonating trusted colleagues or authorities.
- *“Hacktivists.”* Politically motivated hackers might seek to compromise data system security for attention. These individuals attempt to expose security issues or damage the reputation of education agencies they perceive to be easy targets.
- *Malware and ransomware*. Computer programs intended to corrupt or take control of secure systems can put education data at risk.

Vulnerabilities
A number of factors make schools and education agency offices vulnerable to security threats, including the following:

- *Old or unpatched software*. Computer programs that have not been kept up to date might have unaddressed security gaps.
- *Machines without adequate security*. Computers might lack firewalls or other security measures to prevent unauthorized access.
- *“Internet of Things.”* The proliferation of office and classroom equipment capable of connecting to the Internet increases the potential avenues for cyber attacks. Internet-connected devices might include printers, whiteboards and projectors, surveillance systems, and access card readers.
- *Unused equipment*. Discarded or forgotten computers, servers, and other hardware might still provide access to sensitive information.

Although electronic records are more prevalent in education agencies today, paper records also can be at risk of unauthorized disclosure.

Although electronic records are more prevalent in education agencies today, paper records also can be at risk of unauthorized disclosure.

How to Secure Education Data

Safeguarding sensitive data requires preparing for potential incidents with good processes, people, and methods. Education agencies and their employees can take a number of steps at both the organizational and individual levels to secure data.

At the organizational level
Agency leaders and information security (IT) teams can use the following practices and policies to improve data security throughout the organization:

- *Determine the risk*. Perform a risk assessment to identify threats and the organization’s risk threshold. Adopt a “hacker” mindset to find and test vulnerabilities.
- *Develop a data security policy*. The data security policy outlines essential procedures for managing data. Engaging agency leaders in creating the policy will help obtain their support and give the policy authority.
- *Create an incident response plan and identify a response team*. Develop a set of procedures for responding to a security breach. The plan should include steps to be taken in the event of a breach, staff roles and responsibilities, and necessary resources.[*] The incident response team should include both IT and non-IT staff members.
- *Engage employees*. Provide training for the incident response team and for all staff members so that they understand proper data management and security measures. Communicate with employees regularly about security updates and potential risks.

[*] For additional information about incident response plans, see PTAC’s Data Breach Response Checklist, *https://studentprivacy.ed.gov/resources/data-breach-response-checklist*

At the individual level
All education agency employees and data users can adopt practices that will minimize the risk of a breach, including the following:

- *Take advantage of technological solutions*. Encryption, whether applied to individual files or all files on a machine, can make it more difficult for unauthorized users to access sensitive information. Consider requiring WPA2 encryption for wireless networks and using virtual private networks (VPNs). Use screen-locking features on devices, set strong passwords, and install software updates and patches regularly.
- *Practice safe behaviors*. Treat all wireless internet networks as though they are unsecured. Do not join new networks automatically, and beware of issues such as frequent disconnects, slow performance, or warnings. Turn off wireless network connections on devices when they are not needed. Visually check that websites are secure before entering information, and do not open unrecognized links in emails or documents. Do not connect unfamiliar USB drives or devices to computers.

Assessing the Effectiveness of Data System Security

Even with plans and procedures in place, no organization has the resources to be completely secure from a data breach. Rather than waiting to respond to an incident, education agencies must prioritize finding and addressing vulnerabilities in their systems.

Calculate the risk
Risk is measured with three factors: threats, vulnerabilities, and consequences. To calculate the risk of a data security incident, match potential threats with the system vulnerabilities that they could exploit and determine the likelihood that such an incident could occur. Then determine the severity of the impact, or consequences, that would result from the incident.

Risk = Threat x Vulnerability x Consequences

Based on these calculations, identify the potential incidents that are most risky and focus resources on addressing those threats and vulnerabilities. It might be helpful to prioritize risks using a pyramid structure, with the most likely incidents in the bottom tier and the least likely incidents at the top (see figure 1).

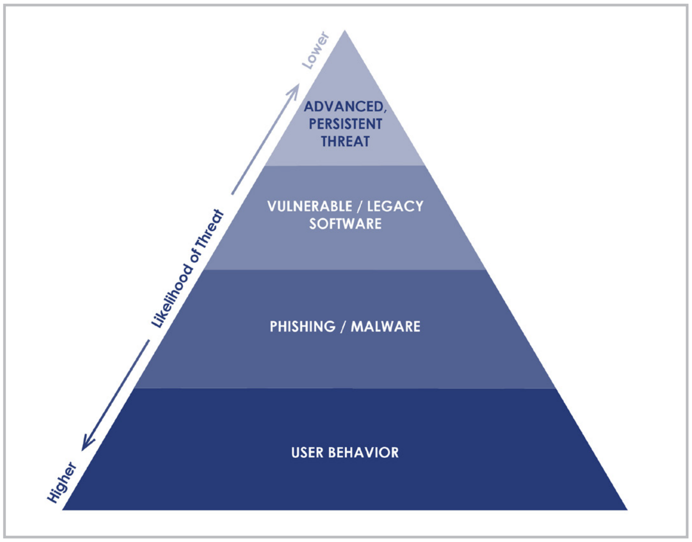

Figure 1. Example risk assessment pyramid with threats arranged according to likelihood

Evaluate and enhance the agency's capabilities
Agencies need to continually review and test their data systems and security measures to address vulnerabilities and minimize threats. The following steps can help sustain security practices and identify potential issues before they result in a major incident:

- *Understand what the agency has*. Take a regular inventory of data systems and the data that they contain. Identify every device within the agency that connects to the Internet. These components all represent targets that might be vulnerable to attack or accidental breaches. Be aware of changes to the "attack surface" that might increase the agency's vulnerability. Ensure that devices no longer in service are cleared of any files that might contain personally identifiable information or other sensitive data. As a best practice, the agency's security policy should limit the storage of PII on local computers and devices.
- *Think like a hacker*. Examine data systems, networks, and hardware from a hacker's perspective to identify and address risks. Hackers often approach targets in five stages: (1) reconnaissance, (2) scanning for vulnerabilities, (3) gaining access to the system, (4) maintaining access to the system, and (5) covering their tracks. Consider ways to disrupt the process so that potential attackers never reach steps 3 through 5.
- *Conduct penetration tests*. Security staff can stage mock attacks on data systems, phishing scams, and other exercises to test security measures and policies. These tests reveal weaknesses for the agency to address.
- *Take advantage of available tools*. Understand the security features available to manage devices and access to information. Several free or low-cost tools are available to help monitor who uses internet-connected devices and how.
- *Minimize human risk factors*. Conduct periodic security training for staff members, including exercises that simulate breaches so that employees can practice putting policies and procedures into action.

Implement practices that reduce the chance for human error, such as avoiding the use of USB drives to share files.

Conclusion

The landscape of education data systems and threats to data security are constantly changing. No amount of policies or resources can protect an organization entirely from the risk of a data breach. However, education agencies have a duty to minimize the risk of security incidents and to respond appropriately if one does occur. Data security teams need to think proactively about system vulnerabilities, potential threats, and the likely consequences of security incidents. By carefully monitoring their technical environments, implementing strong policies and procedures, and engaging staff members, education agencies can reduce the chance of data breaches and better safeguard the privacy of their students and employees.

Additional Resources

Privacy Technical Assistance Center (PTAC) Data Breach Response Checklist
https://studentprivacy.ed.gov/resources/data-breach-response-checklist

PTAC Data Breach Response Training Kit
https://studentprivacy.ed.gov/resources/data-breach-response-training-kit

PTAC Data Security Checklist
https://studentprivacy.ed.gov/resources/data-security-checklist

PTAC Data Security Threats: Education Systems in the Crosshairs
https://studentprivacy.ed.gov/resources/data-security-threats-education-systems-crosshairs

PTAC: W-2 Phishing Scam
https://studentprivacy.ed.gov/resources/w-2-phishing-scam

U.S. Department of Education Student Privacy Website
https://studentprivacy.ed.gov/