FACT SHEET

Ransomware Attacks and the Importance of Collaboration in District-Level Cybersecurity Risk Management

READINESS AND EMERGENCY MANAGEMENT FOR SCHOOLS TECHNICAL ASSISTANCE CENTER

Cybersecurity remains a critical concern for school systems nationwide, as highlighted by the State Educational Technology Directors Association's (SETDA) 2023 State EdTech Trends report and statistics from the K12 Security Information eXchange (K12 SIX) showing a consistent increase in publicly disclosed K–12 cyber incidents over the past 5 years. The U.S. Department of Homeland Security's 2024 Homeland Threat Assessment underscores this trend, predicting ongoing targeting of K–12 school networks by cyber actors who will continue to seek access to school networks, noting that "K–12 school districts have been a near constant ransomware target due to school systems' IT budget constraints and lack of dedicated resources."[1]

Ransomware attacks pose a significant threat to K–12 school districts, disrupting operations, compromising sensitive student and staff data, incurring substantial recovery costs, and eroding the public's trust of schools. An information technology (IT) department, a crucial component to mitigating risks, can implement robust cybersecurity measures and maintain operational continuity.

This fact sheet guides administrators, educators, support staff, and IT staff through the prevention, response, and recovery stages of a ransomware incident at the district level. It also highlights tested strategies and the importance of collaboration with key stakeholders.

SETDA defines Ransomware as "malicious software downloaded from phishing emails or infected websites [that] encrypts data or restricts access to computers to extort money from the victim."[2]

Cybersecurity Organizations to Know

SETDA is a national nonprofit association representing U.S. state and territorial educational technology and digital learning leaders. SETDA builds partnerships and equips its members to leverage technology in support of the education community through advocacy, resources, programs, and initiatives. This includes actively monitoring cybersecurity and privacy trends and fostering communities of practice. These efforts help state education agencies effectively support school districts by enhancing cybersecurity awareness and addressing threats.

K12 SIX is a national nonprofit organization created to safeguard the U.S. K–12 community from emerging cybersecurity threats. Through its Information Sharing and Analysis Center, K12 SIX supports its member organizations with cybersecurity data and intelligence, collaboration opportunities, trainings on addressing cyber threats, technological process solutions, and crisis management.

[1] SETDA-SmallDistrictCybersecurity-October2023.pdf
[2] See SETDA's 2022 Cybersecurity Policy Brief for definitions of common cybersecurity terms.

READINESS AND EMERGENCY MANAGEMENT FOR SCHOOLS
REMS
TECHNICAL ASSISTANCE CENTER

FOR MORE INFORMATION

☎ (855) 781-REMS (7367) ✉ info@remstacenter.org X @remstacenter 🌐 https://rems.ed.gov

ROLE OF IT DEPARTMENTS IN ENSURING OPERATIONS

A school or school district's IT department ensures the integrity, availability, and confidentiality of its data and systems. Key responsibilities include

- **Monitoring**: Continuously monitor systems for cyber threats.
- **Updating**: Keep all software and systems up to date with the latest security patches.
- **Training**: Conduct regular cybersecurity training for staff and students.
- **Backup**: Implement and regularly test data backup and recovery procedures.
- **Incident Response**: Develop and maintain an incident response plan.

IT specialists play a variety of roles in school safety efforts at the state and local levels. Learn more about the ways IT specialists help schools and districts prevent, protect from, mitigate, respond to, and recover from cyber incidents and other emergencies with REMS TA Center's webinar, Understanding the Role of Information Technology Specialists, and the accompanying resource list.

THE ROLE OF SUPERINTENDENTS IN ESTABLISHING A PROACTIVE APPROACH

Superintendents are responsible for the educational and operational administration of their schools, and for communicating strategic priorities to the school community. In collaboration with IT departments, superintendents can promote effective cybersecurity risk management through awareness and a proactive posture. Superintendents must prioritize education and awareness around cybersecurity issues. Superintendents of smaller districts play an especially important role in cybersecurity initiatives, as they are often the first to receive key communications and to actively participate in informational sessions hosted by state education agencies (SEAs) on the topic of cybersecurity. They also often lack dedicated IT staff, and therefore rely on SEAs to help their district remain informed. Proactive engagement helps ensure better preparation, resource allocation, and policy development to strengthen digital security postures.[3]

To develop effective cyber security policies and procedures, it is essential for superintendents to work closely with Chief Technology Officers, Chief Information Officers, applicable school staff, and community-based cyber partners. Collaboration supports

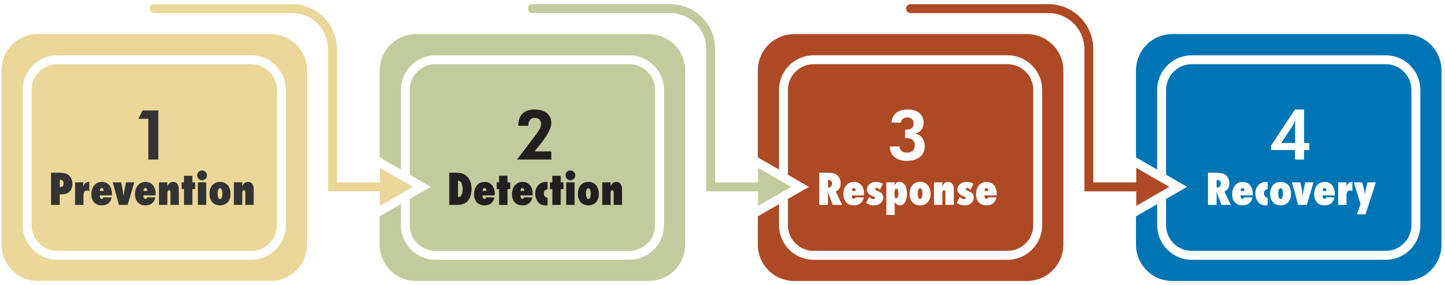
- **Policy Development**: Crafting comprehensive cybersecurity policies and incident response plans.
- **Resource Sharing**: Sharing best practices, tools, and resources.
- **Support Networks**: Establishing support networks for quick response and recovery.
- **Training and Awareness**: Conducting joint training programs and awareness campaigns.

To learn more about the central role of superintendents in overseeing emergency operations plan development and implementation in collaboration with IT department directors and other school district and community partners, watch the REMS TA Center's webinar [The Role of Superintendents in School Safety Efforts](#).

[3] https://drive.google.com/file/d/1xFzytKS6gtFAiKstP_H3ES_Tpm9OF8l8/view?usp=sharing

PLEASE NOTE: The tools and resources identified in this document are not intended as endorsements and are merely offered as examples that you may consider in your own planning efforts.

Ransomware Incident Walkthrough



- **Awareness Programs**: Conduct regular training sessions to educate staff and students about phishing attacks and safe internet practices.
- **Security Measures**: Implement advanced endpoint protection, email filtering, and firewall configurations.
- **Regular Updates**: Ensure all systems and software are updated with the latest security patches.

- **Anomalies Monitoring**: Use intrusion detection systems and security information and event management systems to identify unusual activities.
- **Immediate Alerts**: Set up automatic alerts for any suspicious activity.

- **Incident Response Team**: Assemble a dedicated team to handle the incident.
- **Containment**: Isolate affected systems to prevent the spread of ransomware.
- **Communication**: Inform all stakeholders, including staff, students, parents, and law enforcement agencies, about the incident.
- **Assessment**: Evaluate the extent of the damage and identify the strain of ransomware.

- **Data Restoration**: Use backups to restore affected data and systems.
- **System Clean-Up**: Ensure all malware is completely removed from the systems.
- **Post-Incident Analysis**: Conduct a thorough review of the incident to understand the failure points and improve future responses.

TESTED STRATEGIES FOR ENSURING CYBERSECURITY

1. **Regular Backups**: Maintain frequent and secure backups of critical data, ensuring backups are stored offline.
2. **Endpoint Protection**: Utilize comprehensive endpoint protection solutions to safeguard all devices connected to the network.
3. **Multi-Factor Authentication (MFA)**: Implement MFA to add an extra layer of security.
4. **Network Segmentation**: Segment the network to limit the spread of malware.
5. **Regular Audits**: Conduct regular security audits and vulnerability assessments.

PLEASE NOTE: The tools and resources identified in this document are not intended as endorsements and are merely offered as examples that you may consider in your own planning efforts.

PERTINENT RESOURCES FOR LOCAL EDUCATION AGENCIES

- **National Institute of Standards and Technology (NIST)**: Provides a Cybersecurity Framework that sets guidelines for educational institutions.
- **Cybersecurity and Infrastructure Security Agency (CISA)**: Offers resources, tools, and services for enhancing cybersecurity.
- **Multi-State Information Sharing and Analysis Center (MS-ISAC)**: Provides threat intelligence and cybersecurity resources tailored for state and local government entities, including the education sector.
- **Consortium for School Networking (CoSN)**: Offers tools and resources specifically for K–12 institutions to enhance cybersecurity.
- **Federal Bureau of Investigation (FBI)**: Provides guidelines on handling ransomware incidents and reporting cybercrimes.
- **SETDA Open Educational Resources (OER) Commons Cybersecurity Resources**

CONCLUSION

Superintendents and IT departments play a joint role in prioritizing cybersecurity to protect sensitive data and ensure operational continuity. When superintendents lack awareness regarding the risks and potential consequences of cyber incidents, districts often slip into a reactive position. Given the reliance on digital systems for various operations, from teaching to transportation, districts that take a reactive stance to cyberattacks risk losing valuable instructional days. By understanding and implementing prevention, response, and recovery strategies; taking a collaborative approach, and making use of the resources provided throughout this factsheet, superintendents and IT departments can enhance the resilience of their schools and school districts against ransomware attacks.

For more information on cybersecurity preparedness for K–12 schools, go to https://rems.ed.gov/Cyber.

READINESS AND EMERGENCY MANAGEMENT FOR SCHOOLS
REMS
TECHNICAL ASSISTANCE CENTER

☎ (855) 781-REMS (7367)
✉ info@remstacenter.org
𝕏 @remstacenter
🌐 https://rems.ed.gov