SOUTH CAROLINA
DEPARTMENT OF EDUCATION

MEMORANDUM

TO: District Superintendents
District Technology Coordinators

FROM: Tj Rich, Chief Information Security Officer
Dan Ralyea, Chief Information Officer

DATE: February 5, 2025

RE: Breach Notification and Cybersecurity Best Practices

The recent cybersecurity breach affecting one of our school districts underscores the growing cybersecurity threats facing our schools and the critical need for proactive measures to safeguard our systems and sensitive data. To help prevent similar attacks, we strongly encourage all districts to review and implement the following cybersecurity best practices.

Train Staff and Students on Cyber Threats

- Educate users to recognize and report potential ransomware or malware attacks.
- Conduct ongoing phishing simulations and cybersecurity awareness training.

Implement and Monitor Endpoint Protection Tools

- Ensure all endpoints (computers, servers, and devices) are secured with advanced detection and response (EDR/XDR) tools.
- Regularly verify security tools function and threat detection indicators are updated.
- Promptly investigate and respond to any security alerts.

Strengthen Network and Firewall Protections

- Monitor network activity for unusual data transfers that could indicate a breach.
- Disable unnecessary ports, services, and protocols to minimize vulnerabilities.
- Keep firewall security features and software fully patched. Restrict rule modifications to authorized personnel.
- Log firewall events in a separate, monitored system.

Secure User Accounts

- Require complex passwords that must be reset frequently and not reused.
- Where possible, require multi-factor authentication (MFA).
- Use Virtual Private Networks (VPNs) and MFA for remote connections.

Control Network Access to Prevent the Spread of Threats

- Segment networks using Virtual LANs (VLANs) to limit access to sensitive systems.
- Continuously monitor user and system behavior for anomalies that may indicate a breach.

Maintain Secure and Reliable Backups

- Ensure that backup systems are isolated from your main network to prevent ransomware from spreading.
- Regularly test backups to confirm they are working and critical data can be restored quickly in case of an incident.

Maintain an Updated Incident Response Plan (IRP)

- Keep contact information for key technology and operations leaders current.
- Regularly update response procedures to contain potential threats, including a plan for disconnecting affected systems if necessary.
- Develop contingency plans to continue operations if critical data or systems become inaccessible.
- Conduct regular IRP reviews and training exercises with relevant staff.

Participate in South Carolina Critical Infrastructure Cybersecurity (SC CIC) Program

- Sponsored by SLED, SC CIC provides free cybersecurity intelligence, assessments, phishing training, and incident response support. You can learn more and join SC CIC at the their website.

If your district needs assistance in evaluating its cybersecurity framework and identifying next steps, please do not hesitate to reach out to the Information Security Division (tjrich@ed.sc.gov) at the South Carolina Department of Education. Thank you for your continued commitment to protecting our schools and student data.