OCTOBER 2024 ISSUE • Vol 15

IKON INSIGHTS

TECHNOLOGY NEWS FOR K-12 SCHOOLS

Brought to you by IKON EduTech Group, Inc.

IN THIS ISSUE

This monthly publication provided courtesy of IKON EduTech Group.

IKON is a premium IT consulting company focused on providing K-12 schools with customized technology solutions and personalized support.

Get More Free Tips, Tools and Services on Our Website:
www.ikonbusinessgroup.com
(212)334.6481

3 KEY STRATEGIES TO SAFEGUARD SCHOOLS FROM CYBER THREATS

October marks Cybersecurity Awareness Month, making it the perfect time for schools to strengthen their defenses against cyber threats. K-12 schools are frequent targets for cyberattacks, and the stakes are high. At IKON EduTech Group, we help schools build robust cybersecurity programs aligned with the NIST Cybersecurity Framework and industry best practices.

Here are three actionable steps schools can take right now:

1. INVEST IN HIGH-IMPACT SECURITY MEASURES

With limited resources, schools must prioritize the most effective defenses.

- **Implement Multi-Factor Authentication (MFA):** Add an extra layer of security by requiring more than just a password. Start with administrators and other high-privilege accounts. Use CISA's MFA Enhancement Guide to get started.
- **Keep Software Updated:** Regular patching prevents many attacks. Prioritize known vulnerabilities listed in CISA's catalog. Sign up for free vulnerability scanning reports to stay ahead of potential threats.

(continued on page 2)

3 KEY STRATEGIES TO SAFEGUARD SCHOOLS FROM CYBER THREATS

(continued from page 1)

- **Back-Up and Test Data:** Regularly back up critical data and store it separately from the operational network. Test your backup system frequently to ensure you can recover quickly from any attack.

2. MAKE THE MOST OF LIMITED RESOURCES

Not all security measures require significant spending.

- **Use Free or Low-Cost Tools:** CISA offers a Cybersecurity Services and Tools catalog with resources to detect threats and respond quickly. These can fill gaps in your school's security.
- **Expect More from Vendors:** Don't pay extra for essential security features like MFA or logging. Ensure your vendors enable security by default, and review their hardening guides for further protection.
- **Consider Cloud Solutions:** On-premises IT systems can be expensive to maintain. Moving to secure cloud services, like Google Workspace or Microsoft 365, reduces costs and improves resilience.

3. COLLABORATE AND SHARE INFORMATION

Schools should work together to stay ahead of cyber threats.

- **Join Local Cybersecurity Groups:** In New York State, schools can benefit from joining the Multi-State Information Sharing and Analysis Center (MS-ISAC). MS-ISAC provides critical alerts, free cybersecurity tools, and 24/7 incident support specifically tailored to New York's public sector. By collaborating with this network, schools stay ahead of threats and gain access to valuable resources for threat mitigation and response.
- **Connect with State and Federal Experts:** Build relationships with New York State Education Department (NYSED) cybersecurity experts, local FBI field offices, and CISA (Cybersecurity & Infrastructure Security Agency) advisors. These partnerships give New York schools fast access to federal and state-level support during a cybersecurity incident, ensuring prompt assistance to minimize damage and protect student data.
- **Create and Test an Incident Response Plan (IRP):** Develop an IRP that outlines what to do before, during, and after an attack. Review the plan regularly to ensure it's up to date.

TAKE ACTION NOW DURING CYBERSECURITY AWARENESS MONTH

October is the perfect time to strengthen your school's cybersecurity. IKON EduTech Group can guide you through these key strategies—from MFA implementation to creating an incident response plan. Don't wait for a breach to take action.

ON-DEMAND WEBINAR:
SAFE WEB BROWSING AND DATA LOSS PREVENTION WITH RED ACCESS

Unprotected browsing isn't just a minor issue; it's an open door for data breaches, ransomware, phishing attacks, and unauthorized data sharing with generative AI platforms.

Join IKON Edutech Group and Red Access for a crucial webinar where we address how to secure student browsing activities before disaster strikes.

Watch Now

This session will show you how Red Access's agentless, real-time browsing security keeps students and staff safe while preserving the seamless access needed for education.

ESSENTIAL TIPS FOR FILING FCC FORM 470

The E-rate program provides essential funding for schools. A key step in this process is filing FCC Form 470, the "Description of Services Requested and Certification Form."

WHAT IS FCC FORM 470?

FCC Form 470 initiates the E-rate application process, allowing applicants to briefly describe their institution, provide a contact point, and list specific telecommunications or technology services they need. Once filed, Form 470 is posted publicly, inviting vendors to review and submit bids. It must be posted for at least 28 days before any contracts can be signed, and the next form in the process, FCC Form 471, can be submitted.

ESSENTIAL TIPS FOR FILING FCC FORM 470

1. File Early to Avoid Delays. Timing is Critical: Ensure Form 470 is filed at least 28 days before the FCC Form 471 filing deadline. Filing late could require an FCC waiver, which isn't always approved. Filing early offers flexibility to add or amend requests if needed.

2. Choose Contacts Carefully. Your Primary Contact will handle inquiries from the Schools and Libraries Division (SLD). If another person is better suited for technical questions from vendors, list them as the technical contact.

3. Be Broad in Service Requests. In your Narrative Section, include a comprehensive list of services or products you might need. Listing an item doesn't obligate you to purchase it, but it keeps options open.

4. Include State and Local Procurement Language. Adding relevant procurement requirements helps vendors understand local bidding rules. For NY public schools, purchasing should comply with Sections 103-109 of the State's General Municipal Law and may use centralized or cooperative contracts.

5. Use the RFP Feature in EPC. If needed, utilize the Request for Proposal (RFP) feature to add supporting documents to your Form 470. This could include a formal RFP or a placeholder document stating, "No RFP is being issued." The Adding Addendums feature allows you to post updates, such as Q&A documents for vendor reference.

6. Avoid Naming Preferred Vendors. Stay neutral. E-rate rules mandate an open, competitive bidding process. Mentioning a preferred vendor on Form 470 could lead to application denial.

7. Evaluate Functionally Equivalent Solutions. Although you can indicate manufacturer preferences, fairly consider functionally equivalent alternatives. Add "or functionally equivalent" if listing a specific brand to ensure compliance.

8. Seek Guidance from Peers, Not Vendors. Smaller institutions can ask nearby districts for ideas or post a Request for Info to get suggestions without jeopardizing their E-rate funding. Avoid asking vendors directly, as this may be seen as an unfair advantage.

9. Use "Save and Share" with Caution. The "Save and Share" feature in EPC allows others to access your form, but it transfers control to the other user. To maintain access, share a PDF of the form instead for review.

10. Canceling Form 470. If you need to cancel Form 470, rename the "470 Nickname" to "Cancelled" and create a new form. This keeps the record clear for vendors.

KEY RESOURCES FOR FCC FORM 470

1. **FCC Form 470 User Guide:** Access detailed instructions on the Universal Service Administrative Company (USAC) website: FCC Form 470 User Guide.
2. **Video Tutorials:** USAC offers helpful video tutorials for completing Form 470. View them at USAC's E-rate Webinars.

For more insights on E-rate filing and optimizing technology for educational success, connect with IKON Edutech Group.

INSIDER THREATS IN SCHOOLS: WHY YOUR BIGGEST CYBERSECURITY RISK MIGHT BE FROM WITHIN

When we think about cybersecurity in education, our minds often go to protecting against external threats. But what happens when the risk comes from within? Focusing solely on outside attackers is like double-checking that the front door is locked but leaving the stove on—there's a major blind spot when insider threats aren't addressed.

WHO ARE INSIDERS?

An insider is anyone who has access to your network, data, or physical locations. This includes students, staff, teachers, administrators, and even third-party applications your school may use. They operate within the system, often unintentionally posing risks.

Common unintentional disclosures occur daily, such as:

- A teacher accidentally sending an email meant for one student's parent to another.
- Attaching the wrong student's information to a message.
- Misusing CC instead of BCC when emailing large groups of parents.
- Sending student information home in the wrong backpack.

These are just a few examples, but not all insider threats are accidental. Malicious insiders, whether they seek to harm or simply lack knowledge about data privacy, can lead to significant breaches.

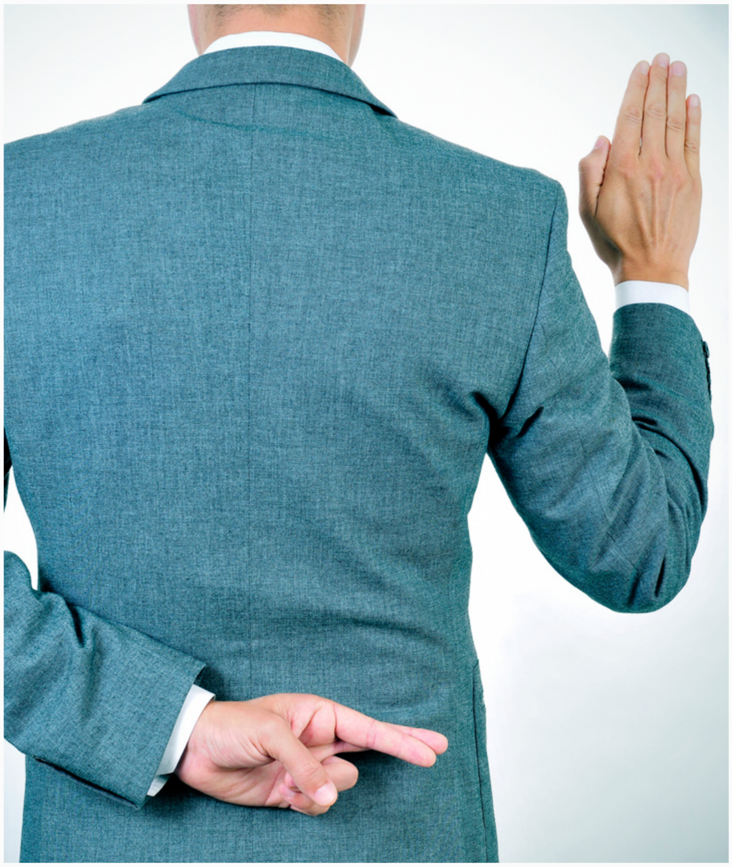
RECENT INSIDER THREAT EXAMPLES

- A student posts unauthorized photos of peers on TikTok.
- A teacher transfers sensitive student data to their personal online account.
- Confidential emails are photographed and shared outside the school.
- A staff member uses parent email addresses for personal purposes.

MITIGATION STRATEGIES

To protect your school from insider threats, consider the following steps:

- **Review Access Permissions:** Implement the principle of least privilege for file and folder access.
- **Monitor Email Rules:** Set up alerts for large attachments or multiple emails being sent outside your domain.



- **Review BYOD Policies:** If devices are provided by the school, assess whether personal device access is necessary.
- **Check Cloud Storage Policies:** Ensure there are strict rules on downloading from platforms like Google Drive or OneDrive.
- **Update Network User Accounts:** Regularly update staff and student access, especially following turnover.

ADDITIONAL SUPPORT

CISA's Insider Threat Mitigation Guide offers excellent insights into strengthening insider threat prevention. One critical recommendation is gaining buy-in across the organization to establish legitimacy for security measures.

By addressing insider threats, schools can better protect their infrastructure, safeguard student data, and minimize both accidental and intentional breaches. Now is the time to look inside and strengthen your internal defenses.