Educate and Take Action: Understand Your School's Cybersecurity Risk

Cybersecurity risk management is a crucial part of every educational institution's overall risk management process. "Cybersecurity is Our Shared Responsibility" is a basic tenet of implementing security. The information below is adapted from the Federal Communications Commission's (FCC) "Ten Cybersecurity Tips for Small Businesses" and reprinted with permission from Deborah A. Snyder, Acting Chief Information Security Officer with the New York State Office of Information Technology Services.

Educate and Take Action:

1. **Train employees in security principles**
   - Establish basic security practices and policies for employees, such as requiring strong passwords and establishing appropriate Internet use guidelines, which detail penalties for violating your school's cybersecurity policies.
   - Establish rules of behavior describing how to handle and protect student information and other vital data.

2. **Protect information, computers and networks from cyber attacks**
   - Keep clean machines. Having the latest security software, web browser and operating system are the best defenses against viruses, malware and other online threats.
   - Set antivirus software to run a scan after each update. Install other key software updates as soon as they are available.

3. **Provide firewall security for your Internet connection**
   - A firewall is a set of related programs that prevent outsiders from accessing data on a private network.
   - Make sure the operating system's firewall is enabled or install free firewall software available online.
   - If employees work from home, ensure that their home systems are protected by a firewall.

4. **Create a mobile-device action plan**
   - Mobile devices can create significant security and management challenges, especially if they hold confidential information or can access official networks.
   - Require users to password-protect devices, encrypt data and install security apps to prevent criminals from stealing information while the device is on public networks.
   - Set reporting procedures for lost or stolen equipment.

5. **Make backup copies of important business data and information**
   - Regularly backup the data on all computers. Critical data includes word processing documents, electronic spreadsheets, databases, financial files, human resources files and accounts receivable/payable files.
   - Backup data automatically if possible, or at least weekly, and store the copies securely, either offsite or in the cloud.

6. **Control physical access to your computers and create user accounts for each employee**
   - Prevent access or use of official computers by unauthorized individuals. Laptops can be particularly easy targets for theft or can be lost, so make sure they are locked up when unattended.
   - Make sure a separate user account is created for each employee and require strong passwords.
   - Administrative privileges should only be given to trusted IT staff and key personnel.

7. **Secure your Wi-Fi networks**
   - If you have a Wi-Fi network for your educational institution, make sure it is secure, encrypted and hidden.
   - To hide your Wi-Fi network, set up your wireless access point or router so it does not broadcast the network name, known as Service Set Identifier (SSID). Password-protect access to the router.

     Do not log into accounts, especially financial accounts, when using public wireless networks.

8. **Employ best practices on payment cards**
   - Work with banks or processors to ensure the most trusted and validated tools and anti-fraud services are being used.
   - You may also have additional security obligations pursuant to agreements with your bank or processor.
   - Isolate payment systems from other less secure programs and don't use the same computer to process payments and surf the Internet.

9. **Limit employee access to data and information, and limit authority to install software**
   - Do not provide any one employee with access to all data systems.
   - Employees should only be given access to the specific data/systems needed for their jobs, and should not be able to install any software without permission.

10. **Passwords and authentication**
    - Require employees to use unique passwords and change passwords regularly.
    - Consider implementing multifactor authentication that requires additional information beyond a password to gain entry.
    - Check with your vendors that handle sensitive data, especially financial institutions, to see if they offer multifactor authentication for your account(s).