States Confront the Cyber Challenge

Cybersecurity in the Education Sector

Educational Institutions Provide Attractive Targets

Although frequently omitted from conversations about cybersecurity, K-12 schools and institutions of higher education are under assault from so-called hacktivists, computer criminals, and nation-states alike. Educational institutions provide a perfect target because they hold much of the same personal, health, and financial information as in other sectors. Theft of this information can lead to financial ruin, reputational damage, and online abuse for students and faculty. Graduate students and their faculty supervisors conduct research into sensitive technologies that nation-state adversaries might want to steal. Many schools own or lease powerful Internet connections that criminal hackers can repurpose to launch sophisticated attacks on other victims.

These computer systems are often vulnerable to compromise. Academic culture, which values open access to information and encourages students to use mobile devices on school networks, creates an enormous attack surface that can be difficult to monitor and secure. Compounding this dilemma are typical challenges such as overworked staff and strapped budgets.

Questions for Governors

- What is the cybersecurity posture of K-12 schools, community colleges, and universities across my state, particularly those involved in sensitive research? Which, if any, maintain written information security policies?
- Do any public universities or K-12 institutions use state information networks?
- Have I convened relevant leadership across the state education enterprise to discuss their current efforts in cybersecurity?
- What is the list of state agencies and officials who have authority to shape cybersecurity in institutions of higher education, and what are they doing in this area?

Recommended Steps for Schools and Governors

Identify current role: Governors and public school officials should evaluate how K-12 and higher education fits into the state's IT governance framework, and make necessary amendments to the framework.

Start with the basics: All schools should develop information security strategic plans that address the security of personal information of faculty, staff, students, applicants, and donors, as well as intellectual property.

Educate school executives: The information security professionals charged with overseeing campus networks are usually well-versed in cyber threats and how to counter them. Their problems often originate with poor coordination and low budgets. Governors should use their convening authority to elevate cybersecurity to the level of school leadership and board members, ensuring their constant engagement with security planning and budgeting.

Emphasize "soft" security: States should consider how to encourage campus-wide initiatives to spread cybersecurity awareness, which does not hinder information sharing and which are fully compatible with educational traditions of openness.

Explore centralization: Governors should convene a summit to determine whether public and private institutions could consolidate the storage of research and intellectual property in a manner that facilitates risk reduction activities while preserving a collaborative environment.

Segment school networks: Any of the thousands of individuals who connect to a university's network—most of whom have not undergone background checks—can potentially access confidential information or cause damage to network systems. Schools can counter this threat at low cost by separating public networks from sensitive ones.

Please e-mail Timothy Blute, Program Director, Homeland Security and Public Safety Division, NGA at: tblute@nga.org *with any questions.*