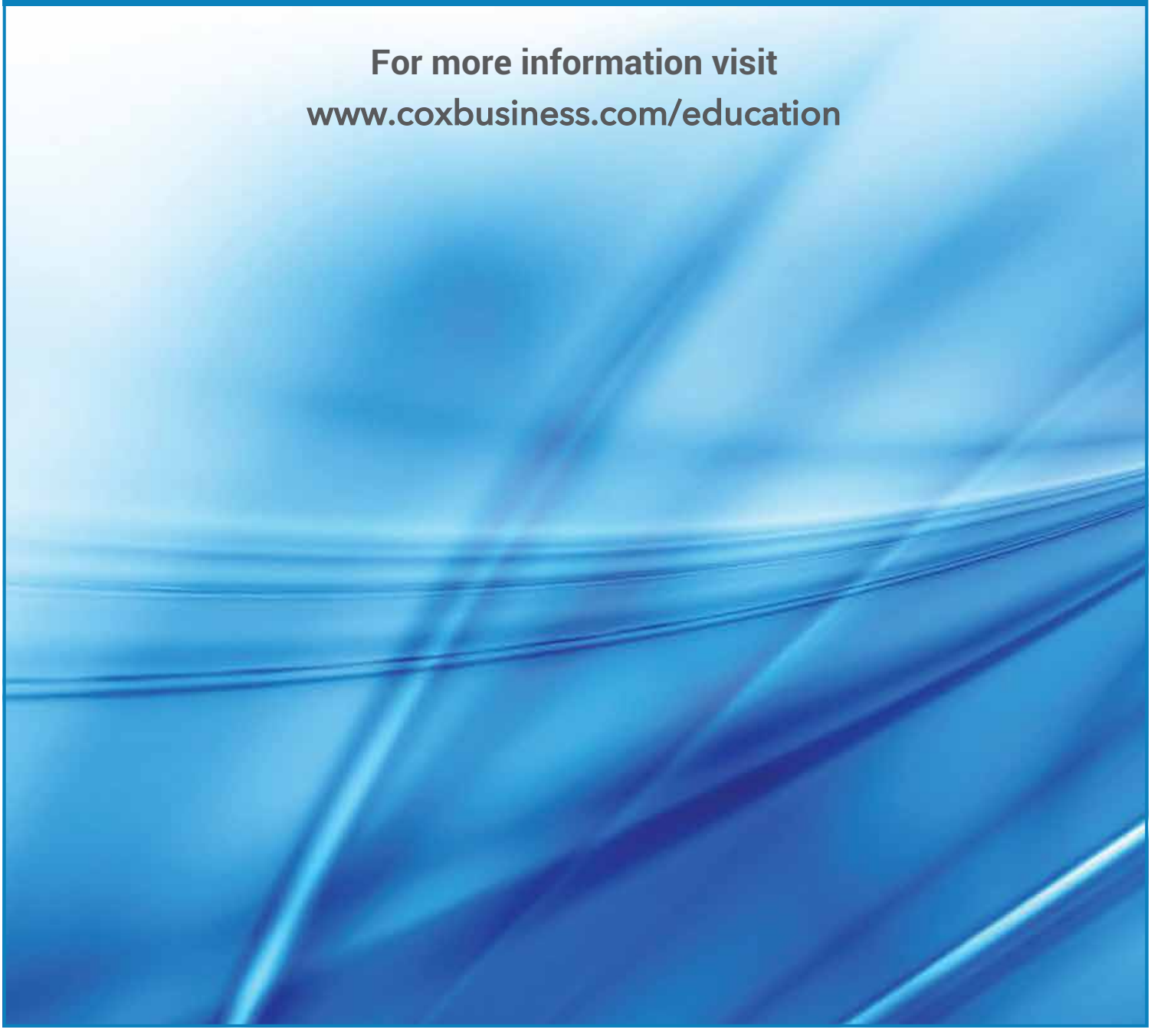
Cox Business®

THE FIVE BIGGEST THREATS TO K-12 NETWORK SECURITY FOR THE 2017-18 SCHOOL YEAR

For more information visit

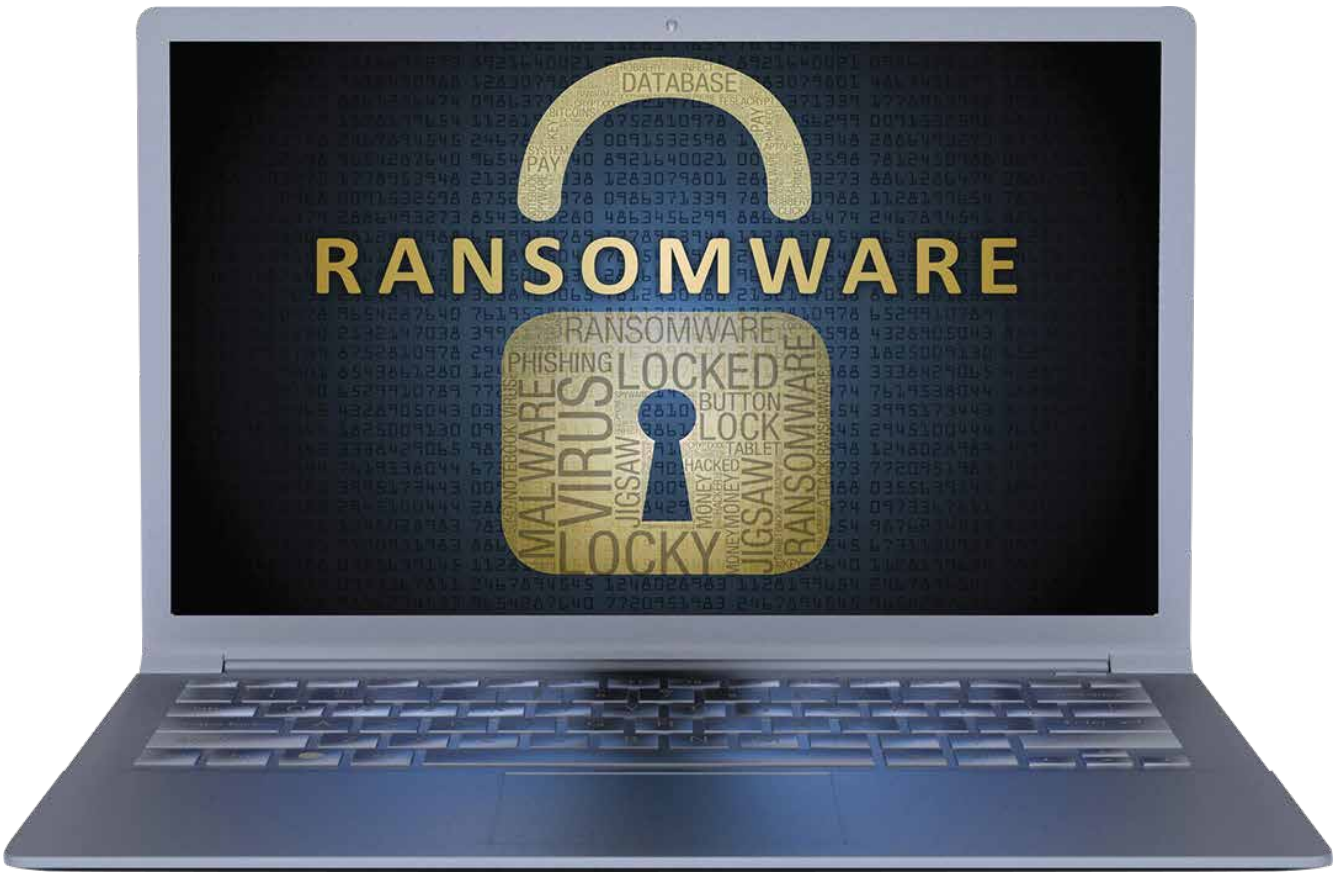
www.coxbusiness.com/education

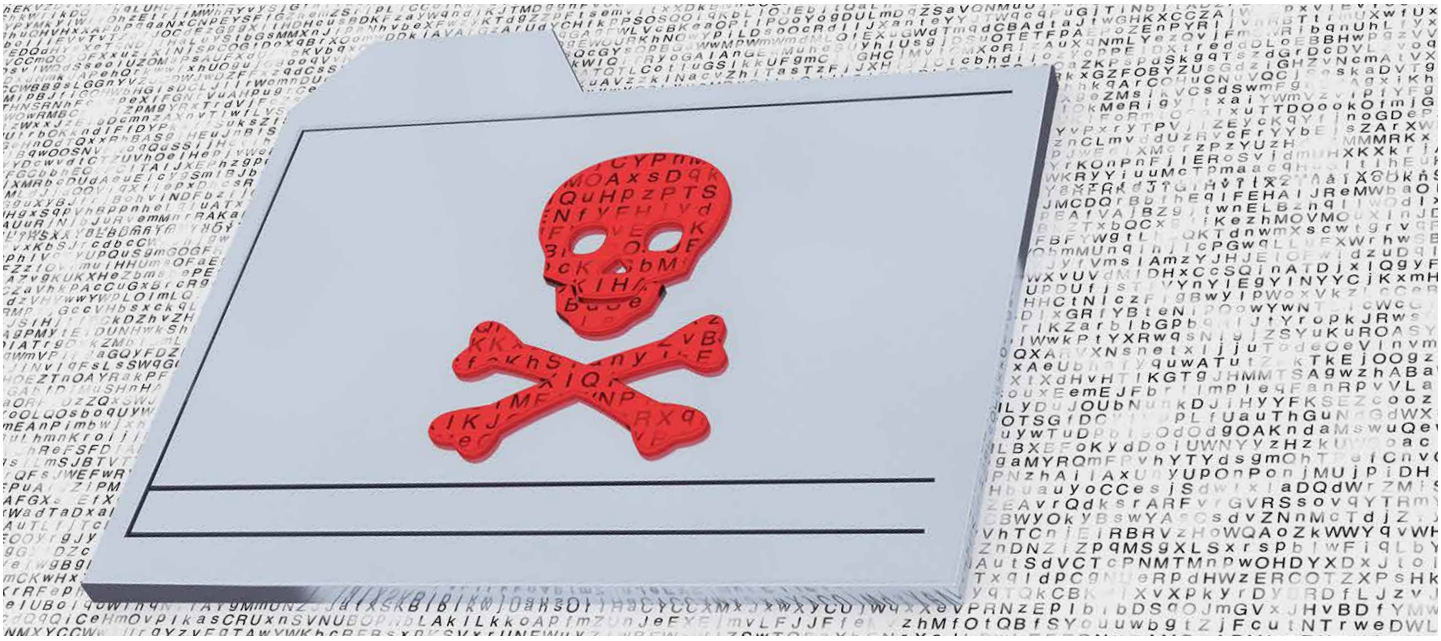


With the current school year winding down, now is a great time for district administrators to start thinking about the improvements that need to be made to the schools in their communities over the summer. If you haven't yet decided where to begin, consider this: in mid-May, schools across the world were victimized by WannaCry, a devastating form of ransomware. Experts believe that this may only be the beginning of a dangerous new trend.

Given the rapidly escalating scale and scope of cyberattacks in the world today, network security must be the top priority for administrators in the new school year. A failure to adopt current security solutions may compromise the fundamental operations that keep your schools efficient and safe.

These are five of the biggest threats to network security facing K-12 school districts in the coming year. By focusing on these key factors, you'll be able to make a smarter decision about where to focus your attention during the summer months full of new projects.





Legacy infrastructure

Outdated infrastructure continues to be one of the greatest threats to ensuring network security today. Maintaining on-premise servers leaves schools vulnerable if their network is compromised. Older hardware may also have security flaws that can be manipulated and used as a foothold to go deeper into your network. Migrating to a cloud-based system will provide a number of benefits, including the protection of student body PII (personally identifiable information).

Cyberattacks

Cyberattacks are the greatest external threat posed to network security. Unfortunately, the scale and complexity of these attacks continues to increase at a torrid pace. But procuring basic antivirus software won't be enough. Instead, you've got to layer your security strategy with advanced and customized solutions that will protect against DDoS, ransomware and a wide variety of other malicious attacks.

Constricted budgets

A lack of funding is certainly a challenge to any administrator interested in beefing up network security. But after most school districts began seeing their funding cut during the 2008 recession, much of that money has yet to make its way back into the education system. This has made it more difficult to acquire top IT talent, as well as patch together an effective network security strategy.

Lack of training

An informed user is one of the most important parts of a successful network security strategy. Unfortunately, many of the people using computers in your schools—students and teachers— are not up-to-date on best practices for maintaining security online. Because your network is only as strong as your weakest link, it is critical to provide your student body with a wealth of resources and training to understand the impact of the actions they take online.

Unsecured technology

Computers, laptops, tablets, phablets and smartphones. Need we go on? The influx of connected technology into your schools is likely to continue again in the new school year. Each of these devices represents an infection point for malware and hackers to enter your network. Don't let the new school year begin without having a series of safety nets in place to secure any new devices connecting to your network.

Cox Business has a broad portfolio of solutions designed specifically for K-12 administrators looking for a cost-effective way to gain total network security. To get started, click here.

COX Business

www.coxbusiness.com/education

1-866-414-7777