The past 15 months have been extremely challenging for every industry, but that is especially true of educational institutions. Every level of education—from local school districts to the largest universities—has had to work to balance the safety of students, faculty and staff with their mission to provide high-quality education all the while knowing that every decision would be highly scrutinized and criticized. During this time of turmoil and uncertainty, many schools faced a challenge they were not expecting – a cyber attack.

Schools collect all sorts of personal and sensitive information about students and parents, making them prime targets for a security breach. In 2020, there were 408 publicly-disclosed data breaches or security attacks in K-12 schools, including student and staff data breaches, ransomware and other malware outbreaks, phishing attacks and a wide variety of other incidents, according to the nonprofit K-12 Cybersecurity Resource Center. This is an 18% increase over 2019. This data does not include cyber attacks at any institutions of higher education, but they are no less susceptible.

As the threat of COVID begins to lift, educational institutions need to shift more of their focus to applying the same preparation and planning as they did for the pandemic to defend against a cyber attack.

**What are some steps educational institutions can take to minimize their risk?**

There are a number of things that educational institutions can do to help limit their exposure to a cyber attack. First, schools — especially colleges and universities where there are more likely to be thousands of personal laptops, mobile phones, tablets and other devices connected to the network — should create, implement and enforce BYOD (bring your own device) policies that address everything from operating system updates to requirements for antivirus and other malware protection (pro-tip: offering free anti-virus software to all users on the system can go a long way in both encouraging and enhancing protection).

Educational institutions should also look into network segmentation if they have not done so already. This way if a cyber attack impacts one part of the network, it may not necessarily impact the whole network. For example, a college could segment the network so that if a hacker was able to access student housing records, the attacker would have no way of accessing student academic or health records.
It’s also important to make sure schools are allocating resources, including personnel, to focus on this issue. For the past year, many schools have understandably shifted their IT spending and employees to focus on expanding their remote learning capabilities. As the world is starting to return to normal, educational institutions need to reallocate at least some of those resources back to protecting from cyber attacks.

As schools examine their resources, they should also take a look at all of their vendor contracts related to IT services or online products. As an example, more schools are turning to third-party “cloud” solutions for data storage and software. While cloud storage has many security advantages, not all providers are created equal, especially when it comes to responding to a security incident. Review contracts to see who is held liable should there be a breach related to a vendor or service and consider renegotiating contracts if needed to limit exposure.

What should an educational institution do if it has been hacked or suspects a cyber attack?

The first thing a school should do is consult its incident response plan. Of course, this presupposes one exists! So, before a school even gets to this point it should develop a robust incident response plan with the help of qualified legal counsel. The benefits of having a plan in place before an incident are substantial. For example, the time-savings and comfort of knowing there are qualified professionals on call to assist can really help make a stressful situation more palatable.

In the event an incident response plan is not in place, consult an attorney who has experience serving as a breach coach and who understands data privacy issues and reporting obligations. While most schools are aware of their privacy obligations under the Family Educational Rights and Privacy Act (FERPA), data breaches that release potentially sensitive information, such as Social Security numbers, have their own legal reporting requirements. For colleges and universities that have students from other states, and even possibly from other countries, reporting gets even more complex as they may be required to meet the legal requirements from every state and country where students live.

Schools should also consider involving law enforcement early in the process—though this decision should be made in conjunction with qualified counsel. Larger jurisdictions sometimes have resources who can help investigate the cause of a data breach. The FBI also has experts who specialize in this kind of work that can be brought in to help with the investigation—especially where there is ransomware involved.

While any online connectivity bears some risk, taking the appropriate steps can minimize an educational institution’s risk of a cyber attack and limit their legal exposure should one occur.