Insights, News & Events

SECURITY BREACHES IN SCHOOLS: 10 STEPS TO PROTECT YOUR INFORMATION

Publication
Jun 3, 2019

California's San Diego Unified School District recently disclosed that it had sustained a data breach when multiple phishing emails from malicious hackers were used to gather login information of staff members throughout the district. The breach exposed Social Security numbers and addresses of more than 500,000 students and staff. The school district is not the first educational institution to fall victim to a cybersecurity breach, and it will not be the last.

According to the Cybersecurity Resource Center, 2018 saw 122 cyberattacks on K-12 educational institutions, averaging out to an attack every three days. But K-12 schools are not the only ones who should be wary of such an attack; institutes of higher learning are being targeted by nefarious cybercriminals on a daily basis as well. One reason that schools are being targeted is that they are repositories for a significant amount of highly confidential information regarding students, parents, staff, and faculty. This includes names, dates of birth, Social Security numbers, mailing and home addresses, phone numbers, billing data, health information, and, in some cases, legal notices.

10-STEP PLAN TO PROTECT YOUR INFORMATION

You should take the steps outlined below to protect your campus communities and make yourself less likely to become the next target of identity thieves:

1. **Enhance School Login Requirements** – Gone are the days when employees can use "1234" or "password" as their password. Instead, require employees to use strong passwords that are complex and hard for hackers to

Related People

Susan M. Guerette
Partner
610.230.2133

Service Focus

Privacy and Cyber

Industry Focus

Education

Higher Education

decipher. Install software requiring employees to change those passwords on a regular basis and prohibiting them from utilizing prior passwords. Consider using "two-step authentication" for particularly sensitive information or for employees who access that information. Also remind employees not to have a "password" file where they store passwords, as those can be hacked as well.

2. **Require Encryption** – Encryption is the process of converting data into another form, or code, so that only people with access to a secret key (called a decryption key) can access the information. Encryption of confidential information should be used wherever that data is stored, such as on files, folders, disks, flashdrives, and the cloud, as well as when information is transmitted, most commonly by email.

3. **Employ A "Need-To-Know" Model** – Data breaches are not always – or even most often – sophisticated attacks through unknown backdoors. Rather, most breaches occur as a result of an employee mistake. You should minimize the risk of this by ensuring that employees are only able to access sensitive information to the extent that it is needed for their jobs. By limiting who can access that information, your school can also limit the likelihood of a security breach.

4. **Train Faculty And Administrative Staff** – Many data breaches happen as a result of employees opening malicious files and attachments or accessing websites that infect their devices. Hackers have become increasingly clever, disguising their malicious software to look like invoices or other files that appear to be coming from reliable vendors. In addition to regular reminders, a useful training tool involves conducting unannounced "fire drills" where fake hacks are sent out to test your employees. By seeing what fake hacks can look like, and being trained to recognize them and question emails before opening them, you will ferret out breaches before they make it to your employees.

5. **Establish Remote Protection** – Your employees may be protected by firewalls and other network security measures while they are on the school campus, but consider measures when your Head of School is traveling or your employees are working remotely from a coffee shop or their homes. Unsecured wireless networks are an area where breaches can occur as data transmitted over

these unsecured channels can be subject to hacking. To address this concern, consult with your IT staff or vendor about using a VPN (virtual private network) for employees to use to access the internet when they are beyond the protection of the campus.

6. **Back Up Your Data** – It is a good practice to consistently back up your data in case there is a system failure. However, don't forget to include security protection measures for the backup system. Cloud backup systems are often forgotten in the security plan and provide an avenue for a data breach. Be sure to conduct audits and test your systems so that any weak spots are detected.

7. **Protect Personal Devices** – While mobile devices offer great benefits, they create risks of infection when unsecured devices are connected to the school's computer systems. In exchange for allowing employees to have the use of these devices at school, be sure to have bring-your-own-device (BYOD) policies and require those devices to have security controls before allowing them to access your protected network.

8. **Include Vendors In Your Process** – Assess whether vendors are storing and transmitting information in a secure and protected manner. Include provisions in agreements with your vendors requiring them to take security measures to protect confidential information and to indemnify the school if their system failure causes a data breach.

9. **Plan Ahead For The Worst-Case Scenario** – Although strong security measures are helpful, a data breach can still happen. You should not start thinking about what you will do about a breach at the first sign of trouble, but should instead already have a data breach response plan. Work with counsel and your IT consultant to ensure that your processes and policies are up to date.

10. **Check Your Insurance Coverage** – Addressing a data breach goes beyond analyzing the breach and how it occurred. The costs include the disruption to your school's mission and managing the disruption and loss of confidence caused by a breach. Your school will also have to notify affected parties of the data breach and offer some type of credit monitoring to those affected. Moreover, you need to prepare for the costs of potential litigation and possible regulatory fines. For these reasons,

make sure your insurance covers the cost of data breaches.

With data breaches on the rise, schools cannot afford to ignore the threat to their campuses. By taking some steps to tighten up their security measures, schools can reduce their risk of exposure and turn back to their main mission of educating students.

For more information, contact the author at SGuerette@fisherphillips.com or 610.230.2133.