12 QUESTIONS

TRUSTEES NEED TO ASK ABOUT DATA SECURITY

Trustees don’t have to be IT experts to secure their institutions — they just need to know the right questions to ask.

By Robert Ferrilli

BACK IN OCTOBER, I HAD THE CHANCE TO SPEAK TO community college trustees from across the country at the 2021 ACCT Leadership Conference in San Diego. It's not always easy to get board members excited about the topic of data security, so I was delighted that the session was well-attended.

I wish I could say it was the *dynamic presenter* that filled the seats, but I know better. Trustees wanted to learn more about the topic because we already knew that 2021 was going to be a record-setting year for data breaches. We were outpacing 2020's total number of events by 17 percent, with no indication this activity would slow in the fourth quarter. If anything, incidences of hacking likely accelerated — and the trend lines will continue pointing up for the foreseeable future.

It's saying something that 2021 was able to match 2020's furious levels of activity, let alone surpass them. After the world went remote and the number of vulnerabilities to exploit exponentially increased, it was hard to imagine that the spikes in nefarious activity were sustainable. Unfortunately, they are — and the implications for higher education are sobering, because colleges and universities are among hackers' favorite targets.

Even before the pandemic, Moody's Investor's Service stated that data security is "a growing risk for higher education institutions globally" because they "retain valuable information across expansive online networks." It went on to note that "their breadth of operations can be vast, with innumerable access points;" and that "investing in state-of-the-art defenses likely competes with myriad other priorities."

In 2021, Moody's doubled down on that stance after the Federal Bureau of Investigation issued a "flash warning" about the growing number of ransomware attacks targeting education institutions — and after one of the largest community college systems in America was forced to delay the start of classes after spring break due to "suspicious activity" in its systems.

Given that ransomware attacks at colleges and universities doubled in 2020; that the average costs associated with those attacks rose to nearly $500,000; and that 2021 will only accelerate these trends, data security is an issue that absolutely demands attention at the trustee level. And as I told that gathering in San Diego back in October, members of the board don't need to know every intricate detail. They just need to know what questions to ask in order to ensure their fiduciary responsibilities are being met — and these 12 questions are a great place to start:

1. **Have we mapped our sensitive data?** Data security begins with knowing precisely where sensitive data is stored and who has access to it. It is the first step in effective data governance.
2. **Do we have a data purge and resting data policy?** Institutions should always purge data that isn't needed — and ensure that resting sensitive data is secure, including records related to former students and employees.
3. **Do we know what regulations and laws apply?** Do you accept financial aid? Are there European nationals among your student body? Do you accept credit cards? All of these activities impact compliance guidelines that should be regularly reviewed.
4. **Do we have an incident response plan?** A step-by-step guide, prepared in advance, can help the team avoid common mistakes in the eye of the storm. Your data breach response plan is every bit as important as those you maintain for disaster recovery and business continuity.
5. **Are our laptops, phones, and tablets encrypted?** These devices are lost by students, faculty, and employees all the time. Proper encryption is the only protection against this inevitability.
6. **Are our computers and devices scanned for vulnerabilities?** Hackers find targets by constantly scanning for vulnerabilities. It's always better to be proactive than reactive and find them first.
7. **Do we ensure that data is transmitted securely?** Email, WiFi, data flows, and even your website can all introduce vulnerabilities if not properly locked down. And everyone needs to know the institution's policies on transmission of sensitive information.
8. **Is multi-factor authentication in place?** Two-factor authentication is a password plus a second authentication method, such as a key or a text message to your phone. It is considered essential practice in data security today.
9. **Are our users password-savvy?** Do students, faculty, staff, and especially administrators know the dos and don'ts of generating effective passwords? Do we have policies in place regarding how often those passwords are changed?
10. **Are our users educated on social engineering?** Do students, faculty, staff, and especially administrators understand how the information they share on social media and other sites can be used against them to create vulnerabilities?
11. **How are we defending against the insider threat?** More than half of all data breaches are generated by people inside the organization. Regular data audits can help protect against an insider attack.
12. **Are we following standard higher education security policies?** Best practices have emerged across the higher education landscape and are the best protection against the new levels of liability that exist.

Trustees don't have to be IT experts to do their part in protecting community colleges against a wave of data loss and theft that is impacting higher education like never before. They just need to know the right questions to ask. What gets watched is what gets done — and by giving data security its proper attention, trustees can ensure that kind of proactivity and preparedness that is needed to weather the storm.

Robert Ferrilli is founder and chief executive officer of Ferrilli Higher Education Technology Consultants. Visit ferrilli.com to learn more.

CREDIT: ILLUSTRATION BY NEIL WEBB