

5 Ways Your LMS Data Management Strategy Exposes Student PII

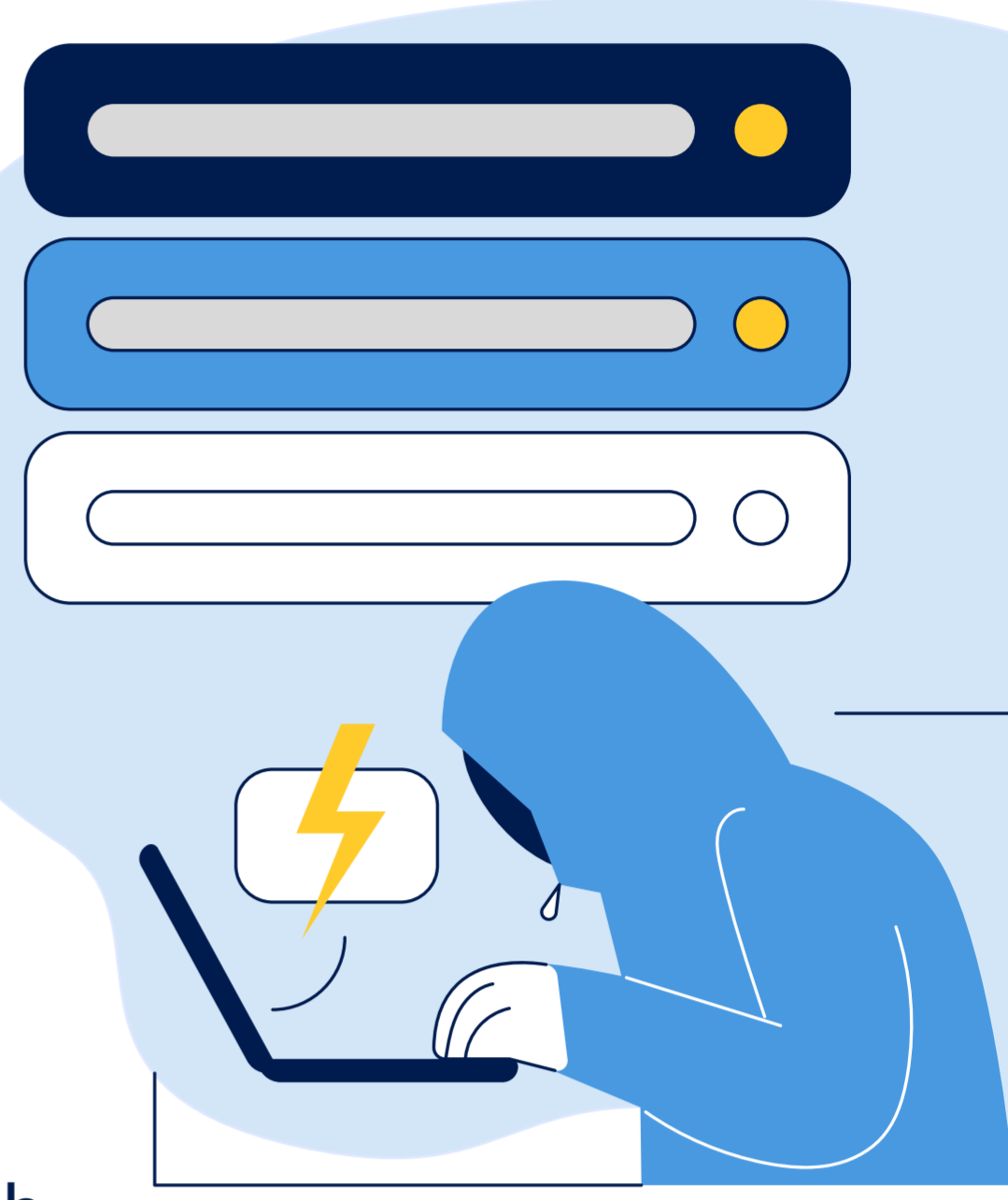
Learning Management Systems (LMS) like [Canvas](#) have become a cornerstone of modern education, allowing institutions to efficiently deliver, track, and manage learning content.

But as these platforms grow in use, so does the amount of sensitive data they hold. From names and email addresses to student IDs, LMS platforms often store a wealth of **Personally Identifiable Information (PII)**. The more data you store, especially over time, the higher the risk of exposure. Here are 6 reasons your institution should carefully manage the PII and student data it stores in Canvas.

1 Increased attack surface with large data volumes

The more data you store on an LMS, the more appealing it becomes to cybercriminals. LMS platforms hold extensive PII, such as student IDs and email addresses, and are prime targets for hackers. With the rise of remote learning, cyberattacks on LMSs have surged.

[IBM reports](#) that the average cost of a data breach reached a record \$4.88M in 2024, a 10% increase from the previous year. A single breach can expose the personal information of thousands, leading to severe financial, legal, and reputational damage.



2 Third-party integrations and data-sharing risks

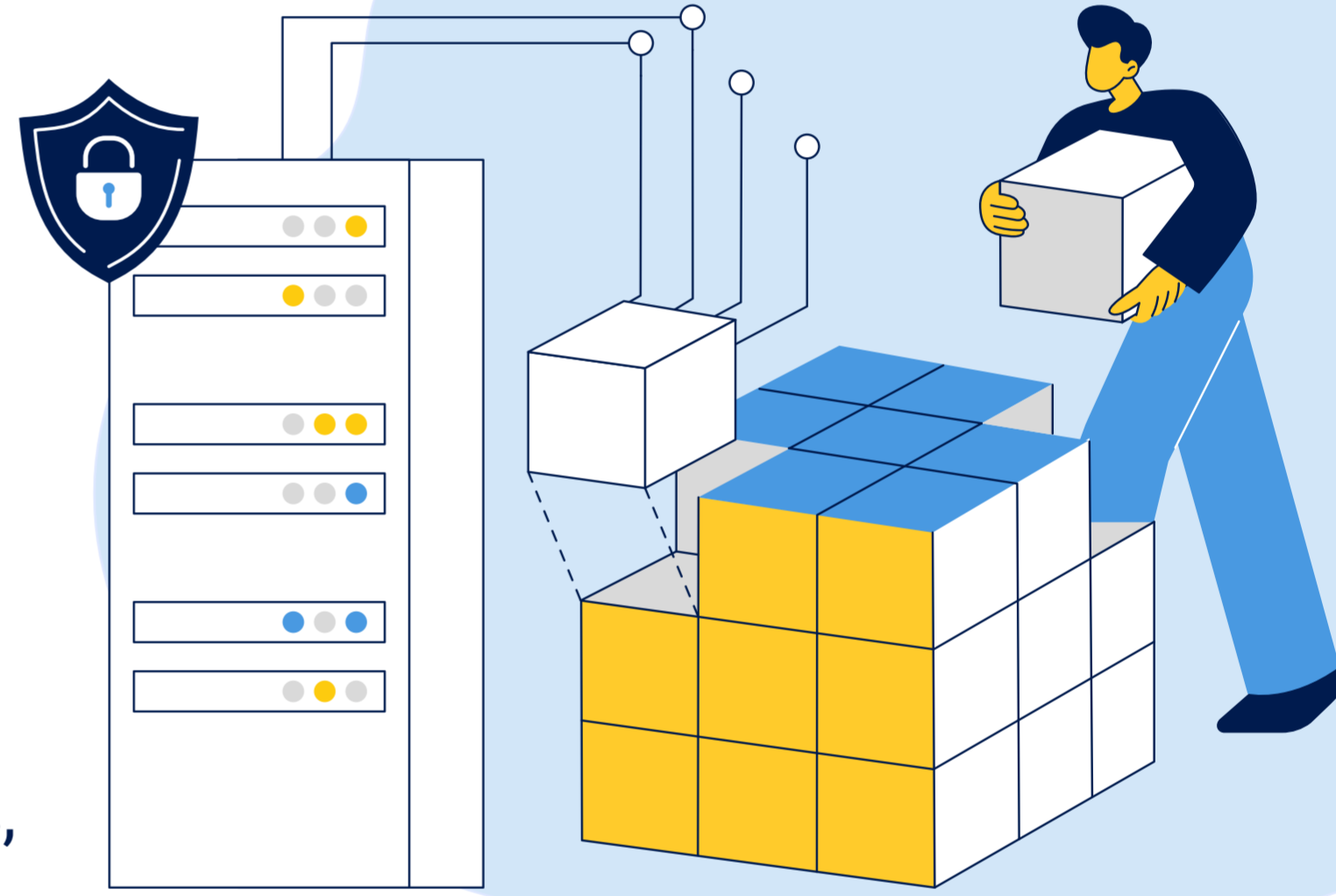
Enhancing your LMS with third-party tools adds valuable features but also introduces risks, especially when sharing PII between systems. Each integration could become a vulnerability if not properly secured. For example, a third-party analytics tool could expose PII stored on your LMS.

To protect sensitive data, ensure all integrations meet the same security standards as your LMS, and reduce the amount of sensitive information left in your LMS.



3 Challenges in data management and deletion

[Managing and securely deleting large amounts of content on an LMS can be complex](#), particularly when PII is embedded in various forms of content, such as documents, discussion forums, or assignment submissions. The decentralized nature of content on an LMS means that PII may be scattered across multiple locations, making it difficult to track and remove when necessary.



4 Access controls for LMS data require a different approach

Basic LMS access controls may not be enough to protect PII. To safeguard sensitive data, you need to implement granular access settings, segregate aging content, or implement an archive solution. This ensures that only authorized individuals can view or interact with specific information, significantly reducing the risk of accidental or unintentional exposure.



5 LMS platforms are not designed for long-term PII management

Your LMS may excel at content delivery and learner management, but it wasn't designed to handle and protect large volumes of sensitive data. While it may offer basic security features, comprehensive PII management requires robust encryption, advanced access controls, and detailed audit trails. [Investing in a specialized archiving solution can bridge these gaps.](#)



Minimize PII risks on your LMS with an archiving strategy

[Canvas Archiving powered by K16 Solutions](#) can be instrumental in managing and protecting PII. By efficiently archiving aging data, you can reduce the volume of sensitive student information stored on your LMS, enhancing security and compliance. [Talk to an archiving expert about how Canvas Archiving can mitigate PII data risks and strengthen your data management strategy.](#)

