How to Secure an **Uncertain Future**

Cloudflare's Dan Kent sees hope in what's to come through new AI solutions, while cautioning higher ed leaders to lock down data to guard against theft as well as data and model contamination.

Seizing all of the opportunities laid bare by artificial intelligence requires colleges and universities to rethink processes and data protections, and at the same time prepare new cyber defenses to ensure accuracy and reliability from the AI models they build. Is higher education ready to take on the challenge? *Campus Technology* recently spoke with **Dan Kent, CTO for Public Sector at Cloudflare**, about the areas where leaders should focus first, as well as the specific tools and solutions that will enable them to construct a solid foundation for future AI initiatives, however they may evolve.

PRODUCED BY: CAMPUS TECHNOLOGY

SPONSORED BY: CLOUDFLARE

"From a cybersecurity risk perspective, there are two key risks which universities need to be aware of and address: data loss and AI-created or -influenced threats and attacks."

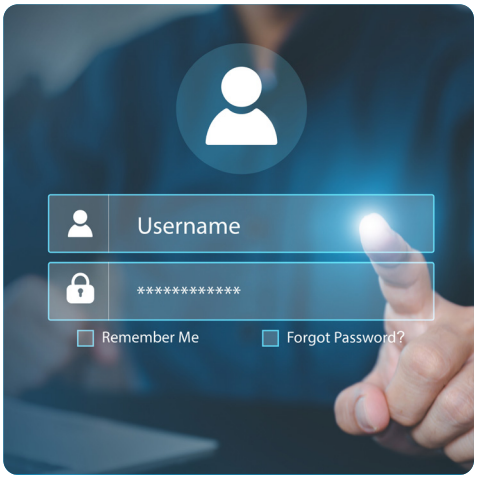
What are the risks for institutions opting to develop and leverage AI tools today in the classroom and for research?

I believe there are two primary risks while looking to deploy and leverage AI tools today: usage risk and cyber risk. As with any new technology, risk will exist and we have to understand that and place guardrails in to limit or mitigate the risk. From a usage perspective, AI tools can be used inappropriately, whether that is a student using AI to perform schoolwork against course policies or a bad actor using AI for more nefarious reasons. Another risk centers around the usage of inaccurate data or hallucinations received from AI models. This can happen due to the quality of data used to train models or due to inherent biases that can be built into the models. Tools such as retrieval-augmented generation (RAG) and large context windows are helping overcome some training deficiencies, and hopefully, over time these biases will be addressed by the model owners through training and other methods.

From a cybersecurity risk perspective, there are two key risks which universities need to be aware of and address: data loss and AI-created or -influenced threats and attacks. Data loss is a real concern when leveraging AI tools if cyber measures such as zero-trust access are not implemented. AI companies leverage tools to scrape websites regularly to assist in training their AI models. Universities should be aware of this practice and make decisions whether to allow that scraping to occur and limit data, or not allow scraping at all. AI prompts are a second area of possible data loss. If students, staff, or admin unknowingly upload sensitive information or PII information into an AI prompt — either purposefully or by mistake — it is possible for that data to be stored and later used to train the AI model. There are preventive measures for this scenario and universities should put those in effect in preparation of this likelihood.

What are the technologies universities should invest in to get the most out of their AI initiatives?

To get the most of their AI investments, it is important to understand how AI will be leveraged by the universities, the staff and the students. To date, much focus in AI has been with the foundational models or LLMs, which rightly deserve focus because they are the 'intelligence' of AI. However, to actually leverage the LLM (beyond just the chatbot), applications will need to be created which work with the



"The best thing a university can do is start with basic cyber hygiene: great asset management and visibility with a comprehensive identity management strategy."

LLM and other tools to create actions, drive workflows, and deliver outcomes. Technologies that can facilitate that end-to-end process need to be leveraged if the university wants to optimize their AI investments. Tools such as AI gateways, which contain cost and provide visibility into how the AI system is running, what LLMs are being used, and to what extent, are imperative. Beyond that, AI firewalls, which can provide guardrails on the AI system and protect the LLM (brain) from improper prompting as well as cyber attacks, will also need to be leveraged.

What can universities do to protect their data from emerging cyber risks around all of this?

The best thing a university can do is start with basic cyber hygiene: great asset management and visibility with a comprehensive identity management strategy. From there, the best data protection strategy can be delivered with deployment of a zero-trust network access (ZTNA) solution. That allows per-application authentication, where the user is only allowed onto the system once the user and the device is verified by context including location, SW versions, security stack etc. Security tools such as secure web gateway (SWG), API gateway, and cloud access security broker (CASB) are all used to ensure data is protected and remains where it should be.

Higher ed appears more open to adopting AI today than other technologies in the past, for instance there was a lot of hesitancy around cloud adoption 10 or 15 years ago.

I think it is great that higher ed is open to AI. Clearly there are risks using AI, just like any new technology, but this is a foundational technology which will impact many fields and industries. Like the internet 30 years ago, AI will bring new business opportunities, productivity in existing fields, and allow creative people to introduce new ideas and capabilities. This technology is moving fast though. I believe universities can help mature the technology in the research arena and help prepare students for the world of tomorrow by using this technology in the classroom and program to help deliver the modern workforce.
