HURON

Five Cybersecurity Considerations for Higher Education CIOs and CPOs

COLLABORATION AND STRATEGIC ALIGNMENT ARE ESSENTIAL FOR SUCCESS

By Jens Brown and Mark Cianca

Technology integration in higher education has created opportunities for improved efficiency but has also introduced new risks. With the increasing popularity of cloud services, the rapid adoption of automation and artificial intelligence (AI), and ever-evolving cyberthreats, it is vital for chief information officers (CIOs) and chief procurement officers (CPOs) to collaborate on ensuring the security and compliance of their technology environment and procurement processes.

Below are five actions to help CIOs and CPOs at colleges and universities select and implement new technology more securely.

Scrutinize Off-Contract Purchases and IT Services

When campus customers circumvent the procurement process, they introduce potential risks that can be difficult to assess and manage. Such risks occur because off-contract products and IT services are typically not subject to the same security standards as those of contracted providers.

Mitigating Risk

CIOs and CPOs must work with their IT security teams to implement a comprehensive cyber risk management program, including conducting regular security assessments and penetration testing, implementing encryption and access controls, and monitoring cyberthreats.

Initial and ongoing security assessments are also necessary to ensure that suppliers of IT products and services establish and maintain a robust cybersecurity posture.

For example, the National Security Agency noted that "cloud services can introduce risks that organizations should understand and address both during the procurement process and while operating in the cloud."

To avoid independent acquisition of products and services by individuals or departments, such as with a credit card, the procurement office must actively drive category management improvements, as noted in the callout box.

Stay Updated on Cybersecurity Threats

In the first half of 2022, cyberattacks in higher education increased by 44% compared to 2021, with an average of 2,297 attacks weekly. Growing and evolving threats make it essential for colleges and universities to employ best practices for mitigation.

Ways to remain vigilant include participating in ongoing cybersecurity training, attending relevant industry events, being aware of the latest threat intelligence, and reviewing industry publications and news sources.

Compliance with industry regulations and standards, such as the General Data Protection Regulation (GDPR), CCPA (California Consumer Privacy Act of 2018), and the Health Insurance Portability and Accountability Act (HIPAA), is essential to data security.

With the federal government continuing to tighten cybersecurity requirements for its contractors, research organizations may need additional precautions to comply with federally sponsored research. The Cybersecurity Maturity Model Certification (CMMC), introduced by the Department of Defense (DoD), is a prime example of such a requirement.

The DFARS (Defense Federal Acquisition Regulation Supplement) is a supplement to the FAR (Federal Acquisition Regulation) that includes additional acquisition regulations specifically for the Department of Defense (DoD). DFARS 252.204-7012 requires contractors to implement the security controls specified in NIST SP 800-171, a set of cybersecurity standards that form the basis of the CMMC framework. DFARS 252.204-7021 and DFARS 252.204-7020 require CMMC compliance for DoD contracts and subcontracts. In addition to the FAR and DFARS, other regulations may apply depending on the specific agency or program sponsoring the research.

Institutions that work with defense contractors or sub-contractors must understand the requirements of the CMMC and other applicable regulations. In addition to facilitating compliance, CIOs and CPOs can play a significant role in driving a culture of cybersecurity awareness, regulatory compliance, and education throughout campus.

Procurement practitioners can integrate cybersecurity education and awareness programs into the process by working with their IT security teams. Educational components can include requirements for cybersecurity training and awareness as part of contract terms and conditions and the inclusion of cybersecurity maturity level requirements in RFPs and other procurement documents.

Secure Automation and AI Solutions

Automation and AI solutions are revolutionizing finance and administration processes in higher education. At the same time, the increasing use of AI in the enterprise has brought new security risks, such as data theft, loss, or misuse, and the risk of biased or discriminatory results. Understanding associated implications and instituting security measures, as noted in the callout box, can help keep these risks at bay.

Taking a risk-based approach to implementation, institutions should stay informed about advancements in automation and AI and proactively incorporate security considerations into procurement decisions.

Manage Cloud Adoption

When implemented securely, cloud services offer colleges and universities the ability to scale their IT infrastructure, improve collaboration, and reduce costs. As a first step, CIOs and CPOs should make procurement decisions based on alignment with the institution's IT architecture, security requirements and policies, and privacy standards.

Consider Cyber Liability Insurance

The financial losses and reputational damage of a data breach or cyberattack can be devastating. Costs for notifying affected parties, legal fees, credit monitoring, and recovering lost data can reach millions. Cyber liability insurance can help protect institutions against loss.

Selecting and implementing new technology can help colleges and universities reach their strategic goals. But when the technology is compromised by a security breach, the resulting damage can reverse any gains. To be successful, institutions should prioritize cybersecurity before, during, and after deployment, beginning with ensuring that the CIO and CPO are working collaboratively to mitigate risk. By working together and investing in cyber risk management programs, CIOs and CPOs can help colleges and universities continue to thrive, innovate, and deliver the best possible technology solutions to their students, faculty, and staff.

HURON

huronconsultinggroup.com