Kiteworks

Higher Education: 2023 Sensitive Content Communications Privacy and Compliance

Industry Findings and Takeaways

HIGHLIGHTS

Communication Tools in Use	**29%**	7+
	38%	6
	24%	5
	10%	Less than 4
Average Annual Budget for Communication Tools	**27.7%**	$500,000+
	21.3%	$350,000 – $499,999
	25.5%	$250,000 – $349,999
	19.1%	$150,000 – $249,999
	6.4%	$100,000 – $149,999
Number of Third Parties With Which They Exchange Sensitive Content	**23.4%**	5,000+
	29.8%	2,500 – 4,999
	29.8%	1,000 – 2,499
	8.5%	Less than 999
Attack Vector Weighted Score (based on ranking)	**100**	Password/Credential Attacks
	81	Session Hijacking
	80	URL Manipulation
	69	DNS Tunneling
	64	Phishing
	59	Denial of Service
	56	Cross-site Scripting
	55	Zero-day Exploits and Attacks
	50	Man in the Middle
	37	Rootkits
	32	SQL Injection
	27	Malware (ransomware, trojans, etc.)
	25	Insider Threats
Exploits of Sensitive Content Communications in Past Year	**14.9%**	10+
	38.3%	7 – 9
	36.2%	4 – 6
	10.6%	2 – 3
Level of Satisfaction With 3rd-party Communication Risk Management	**4%**	Requires a New Approach
	47%	Significant Improvement Needed
	19%	Some Improvement Needed
	30%	Minor Improvement Needed

Higher Education: A Prime Target for Cybercriminals and Rogue Nation-states

Higher education institutions are increasingly falling victim to cyber threats instigated by rogue nation-states and cybercriminals. Kiteworks reveals a 22% spike in incidents from 2022 to 2023 in higher education. An abundance of personally identifiable information (PII) and intellectual property (IP), which includes national and industrial secrets and research data, is a veritable goldmine for these malicious actors. A GAO report last year found that higher education institutions with research contractors connected to the federal government and defense industrial base organizations have a serious risk of sensitive data being shared with the home countries of students and scholars studying at U.S. universities.[1]

Fragmented Tool Landscape Increases CapEx and OpEx

Communication tool disaggregation is one of the contributing factors behind cyber risk in higher education. Kiteworks' 2023 Sensitive Content Communications Privacy and Compliance Report found that 91% of higher education institutions employ five or more tools for managing sensitive content communications. Disparate tools make it immensely more difficult to establish policies to track and control access to sensitive content. For higher education institutions that need to demonstrate compliance, this siloed approach makes it immensely more difficult to confirm adherence with security standards and regulatory compliance. Finally, acquiring and overseeing multiple toolsets escalates capital expenses (CapEx) and operating expenses (OpEx)—with nearly three-quarters of higher education survey respondents indicating they spend $250,000 or more annually on communication tools.

Assessing Third-party Content Communication Risks in Higher Education

Higher education institutions encounter substantial risks related to third-party content communications. Two-thirds use six or more systems to track, control, and secure content communications with third parties, increasing their risk exposure. Moreover, respondents in higher education reveal that file sharing and mobile application communication channels pose the highest risk—communication channels leveraged by research students and scholars, including those from nations with a history of theft of IP and nation-state secrets.

Almost 9 out of 10 higher education respondents experienced four or more exploits of sensitive content communications in the past year, highlighting a significant security concern.

91% of higher education survey respondents say they rely on more than five disparate communication tools, with nearly 75% spending $250,000 or more each year, on average, on them.

At the same time, the breadth of third parties with which higher education institutions exchange sensitive content is substantial: 63% engage with 2,500 or more third parties, escalating the complexity and risk of secure content communication.

All of the above becomes very concerning when the maturity of governance tracking and controls is examined. For example, merely 36.5% have the ability to track and control access to sensitive content folders across all content types and departments. Seven out of 10 survey respondents admit they must enhance their strategies to mitigate risks linked with third-party content communication. This is quite high when compared to other industry responses, an indication that higher education lacks governance maturity. At the same time, it is concerning with 89% experiencing four or more exploits of sensitive content communications in the past year.

Higher Education Must Enhance Digital Risk Management

Nearly one-third of respondents indicate they have policies for tracking and controlling content collaboration and sharing on-premises, while only one-quarter have the same in place for the cloud. Remarkably, only 36.5% of higher education institutions have governance tracking and controls on-premises and in the cloud. PII is seen as the data type posing the highest risk, with almost 40% ranking it number 1 over other data types. These statistics expose a worrisome gap in digital risk management practices within the higher education sector, emphasizing the urgent need for improvement to safeguard sensitive content better.

Kiteworks Private Content Network for Higher Education Institutions

The Kiteworks Private Content Network empowers higher education institutions to share and transmit sensitive content such as student records, research data, faculty correspondence, strategic plans, and administrative documents. With Kiteworks, higher education institutions can share sensitive student information, such as transcripts, financial aid documents, or personal data, with authorized personnel, including third parties. Professors and instructors can securely distribute course materials and resources to students, ensuring that only authorized users can access them. They can also exchange grant applications and funding data with external partners. Faculty members and researchers can collaborate on conference presentations and papers that include sensitive information.

[1] "Enforcement Agencies Should Better Leverage Information to Target Efforts Involving U.S. Universities," U.S. General Accounting Office, June 14, 2022.

Get the Full Report

Kiteworks

Kiteworks 2023 Sensitive Content Communications Privacy and Compliance Report

Seeking to empower private and public sector organizations to manage their file and email data communication risks better, Kiteworks began publishing an annual Sensitive Content Communications Privacy and Compliance Report in 2022. Rogue nation-states and cybercriminals recognize the value of sensitive content and target the communication channels used to send, share, receive, and store it—email, file sharing, managed file transfer, web forms, APIs, and more.

The 2023 Sensitive Content Communications Privacy and Compliance Report surveyed 781 IT, security, risk, and compliance professionals across numerous industries and 15 different countries. The in-depth report, which is based on their survey responses, explores a range of issues related to file and email data communication risks—how organizations are addressing those today and plan to do so in the coming year. The analysis includes a look back to 2022 data and what changes were observed in 2023.

Copyright © 2023 Kiteworks. Kiteworks' mission is to empower organizations to effectively manage risk in every send, share, receive, and save of sensitive content. The Kiteworks platform provides customers with a Private Content Network that delivers content governance, compliance, and protection. The platform unifies, tracks, controls, and secures sensitive content moving within, into, and out of their organization, significantly improving risk management and ensuring regulatory compliance on all sensitive content communications.