Kiteworks

2024 Analysis of Sensitive Content Communications in Higher Education: Security and Compliance Trends

HIGHLIGHTS

Communication Tools in Place	5%	7+
	7%	6
	37%	5
	21%	4
	12%	3
	9%	2
	5%	1
Exchange Sensitive Content With Third Parties	7%	Over 5,000
	40%	2,500 to 4,999
	19%	1,000 to 2,499
	16%	500 to 999
	19%	Less Than 499
Data Types Biggest Concern (Top 3)	58%	PII
	50%	IP
	46%	Financial Documents
	42%	Legal Communications
	35%	GenAI LLMs
	23%	PHI
	23%	CUI and FCI
	23%	M&A
Biggest Privacy and Compliance Focus (Top 2)	49%	CMMC
	44%	U.S. State Privacy Laws
	37%	HIPAA
	35%	SEC Requirements
	23%	GDPR
	12%	Country-specific Data Privacy Laws
	0%	PCI DSS
Most Important Security Validations (Top 2)	63%	NIST 800-171/CMMC 2.0
	60%	ISO 27001, 27017, 27018
	33%	FedRAMP Moderate
	19%	SOC 2 Type II
	16%	IRAP (Australia)
	7%	NIS 2 Directive
Number of Times Experienced Sensitive Content Communications Hack	5%	10+
	51%	7 to 9
	14%	4 to 6
	14%	2 to 3
	2%	1
	14%	Don't Know

The 2024 Kiteworks Sensitive Content Communications Privacy and Compliance Report provides an in-depth analysis of the challenges and trends in managing sensitive content across various industry sectors, including higher education. This brief focuses on the key findings related to higher education, highlighting the tools used for sensitive content communications, cybersecurity concerns, third-party communication risks, specific cyber threats, and compliance implications.

Managing All the Sensitive Content Communications Tools

Almost half (49%) of higher education institutions rely on five or more communication tools to send and share sensitive content, which is slightly less than the full cohort average (53%). When it comes to tracking and controlling sensitive content, only 19% of higher education respondents said they can track and control sensitive data sent and shared internally; an even lower percentage of higher education respondents said they can do so when it is exchanged externally (14%). This is substantially worse than the full cohort averages—51% for internal data exchanges and 43% for external data exchanges.

By far, higher education is at a much higher risk in the governance of sensitive data than other industry sectors. Putting aside personal data (PII and PHI), which is a risk in itself, higher education sends and shares highly confidential data such as national IP and secrets, including research for the U.S. Department of Defense. Due to the sector's abysmal governance results, the risks are tangible.

When it comes to sensitive content communications privacy and compliance priorities, mitigating lengthy and expensive litigation was cited 63% of the time as either their first or second priority. This was followed by prevention of leakage of confidential IP and corporate secrets (56%). These two top priorities reflect the rise of data privacy regulations and their enforcement, as well as the need to protect confidential data, including that exchanged by higher education institutions.

Assessing the Third-party Risk of Sensitive Content

Managing third-party risk is a substantial gap for higher education, with 47% reporting they exchange sensitive content with over 2,500 third parties (slightly higher than the global cohort at 44%) and 66% doing so with more than 1,000 third parties (the same as the full respondent average of 66%). When it comes to tracking and controlling sensitive content once it leaves an application, higher education is one of the more mature industry sectors with 31% indicating they can track and control over three-quarters of sensitive content when it leaves an application.

Assessing the State of Sensitive Content Compliance

84% of higher education respondents revealed their measurement and management of compliance for sensitive content communications requires some to significant improvement. This was slightly less than what all respondents reported: 88%.

The involvement of many higher education institutions in defense industrial base (DIB) matters came out in the question involving what compliance standard is their biggest focus. Higher education respondents listed CMMC 2.0 as their first- or second-highest priority (49%). Next highest was U.S. state data privacy laws (44%)—a reflection on the need to protect PII.

Of the various security standards and validations, higher education respondents choose NIST 800-171 more often than any other one (63%), a likely reflection on the amount of data exchange that occurs with the federal government. A close second was ISO 27001, 27017, and 27018 (60%).

Assessing the Risk of Sensitive Content Security

86% of higher education respondents indicated their measurement and management of security risk associated with sensitive content communications requires significant or some improvement; an additional 2% said they have nothing in place today. Both largely are in the margin of error from the full cohort.

56% of higher education respondents reported their sensitive content was breached seven or more times. This was quite concerning in that the number of breaches is significantly higher than the full cohort (32% said they had seven or more). This is a serious gap that needs to be closed. Higher education is certainly in the crosshairs of bad actors; Verizon's DBIR found that higher education was targeted more often than most industry sectors and that more breaches occurred in higher education than any other industry sector.[1]

Higher education respondents claim they employ advanced security capabilities and practices such as encryption, multi-factor authentication, and governance tracking and control of internal sensitive content communications at a higher rate than other industry sectors (65% compared to 59% for the full cohort).

Assessing the Cost of Security and Compliance

All the data breaches in higher education translate into a higher litigation risk; almost half of all respondents said they spend over $5 million annually in litigation. This was the highest of any industry sector, an indication higher education needs to double or triple down both the security and governance of sensitive content communications. And with 19% of higher education respondents indicating they do not know their data breach litigation cost, the risk is further exacerbated.

Knowledge and Categorization of Data Types

Many higher education respondents indicated they tag and classify over 50% of their unstructured data (79%). Compared to many other industry segments, higher education revealed that they do not believe unstructured data needs to be tagged and classified in high numbers (only 14% said over 60% needs to be tagged and classified).

Imperative for Robust Sensitive Content Management in the Higher Education Sector

The Kiteworks 2024 Sensitive Content Communications Report highlights the critical need for robust management of risk and compliance in sensitive content communications in the higher education sector.

Protecting the personal data of students, faculty, and staff is certainly an important part of the charge of higher education institutions. Thus, it is no surprise that higher education respondents listed personally identifiable information (PII) more often than other data types (58% listed it first or second). Yet, at the same time, protecting sensitive data related to corporate IP and secrets is even more important; 50% of higher education respondents listed it as their first- or second-highest data-type risk.

Operationally, higher education institutions spend a lot of time managing logs generated by the numerous communication tools they use to share and send sensitive content. 58% of respondents must reconcile over 11 (10 percentage points higher than the average of all respondents). 9% of higher education respondents did not know how many logs must be reconciled. Compared to other industry sectors, higher education spends more time aggregating logs used to prep for compliance reports—49% spend 2,000 hours annually on these reports.

[1]"2024 Data Breach Investigations Report," Verizon, May 2024.

Get the Full Report