Innovation Growth Partners Specialty®

CONTACT US

Dave Perkins, RPLU
(508) 848-4263
dave.perkins@igpspecialty.com

Common Cyber Claim Examples for Educational Institutions

K–12 Schools, Private Schools, Colleges and Universities

Educational institutions have become prime cyber targets because they maintain large volumes of personally identifiable information (PII), payment card data, employee records, health information, research data, and financial assets. The following claim scenarios highlight how cyber incidents can create first-party losses, third-party liability, regulatory exposure, and significant operational disruption.

1. Ransomware Shuts Down School Operations

Claim Scenario

A school district is hit by ransomware that encrypts student information systems, payroll applications, transportation scheduling software, and classroom technology. Multiple schools are unable to operate normally for several days.

Potential Costs

- Forensic investigation
- Legal counsel
- Ransom negotiation and payment
- Data restoration
- Public relations expenses
- Extra IT consulting costs
- Business interruption losses

Cyber Coverage Typically Triggered

- Incident Response
- Cyber Extortion
- Digital Asset Restoration
- Business Interruption

2. Student Information Data Breach

Claim Scenario

Hackers gain access to student databases containing names, addresses, Social Security numbers, disciplinary records, and parent contact information.

Potential Costs

- Notification expenses
- Credit monitoring
- Regulatory investigations
- Privacy litigation
- Legal defense costs

Cyber Coverage Typically Triggered

- Privacy Liability
- Regulatory Defense
- Breach Response Costs

3. Employee Payroll Diversion Fraud

Claim Scenario

A phishing campaign compromises employee payroll credentials. Attackers alter direct deposit information for dozens of faculty and staff members before the fraud is discovered.

Potential Costs

- Reimbursement of diverted funds
- Investigation expenses
- Employee relations costs
- System remediation

Cyber Coverage Typically Triggered

- Cyber Crime Coverage
- Social Engineering Coverage
- Funds Transfer Fraud Coverage

4. Business Email Compromise (BEC)

Claim Scenario

A fraudster impersonates the Head of School and instructs the controller to wire $400,000 toward a fictitious capital improvement project.

Potential Costs

- Direct financial loss
- Investigation costs
- Recovery efforts
- Legal expenses

Cyber Coverage Typically Triggered
- Social Engineering Fraud
- Crime Coverage
- Funds Transfer Fraud

5. Tuition and Payment Card System Breach

Claim Scenario
Attackers compromise a college's online tuition payment portal and steal payment card information from thousands of students and parents.

Potential Costs
- PCI assessments
- Card replacement costs
- Class action litigation
- Forensic expenses

Cyber Coverage Typically Triggered
- PCI Coverage
- Privacy Liability
- Breach Response

6. Exposure of Student Health Information

Claim Scenario
An improperly configured student health portal exposes medical records, counseling records, and treatment information.

Potential Costs
- Privacy investigations
- Notification expenses
- Regulatory proceedings
- Legal defense costs

Cyber Coverage Typically Triggered
- Privacy Liability
- Regulatory Proceedings Coverage
- Incident Response

7. Phishing Attack Against Faculty

Claim Scenario
Multiple faculty members unknowingly provide credentials through a phishing campaign, allowing attackers to access grading systems, student records, and email accounts.

Potential Costs
- Forensic investigation
- Network remediation
- Breach notification
- Privacy claims

Cyber Coverage Typically Triggered
- Network Security Liability
- Privacy Liability
- Incident Response

8. Theft of Academic Research Data

Claim Scenario
A university research department suffers a network intrusion resulting in theft of proprietary research funded by government agencies and private sponsors.

Potential Costs
- Forensic response
- Contractual disputes
- Sponsor claims
- Regulatory inquiries
- Reputational harm

Cyber Coverage Typically Triggered
- Network Security Liability
- Security & Privacy Liability
- Incident Response

9. Third-Party Vendor Data Breach

Claim Scenario
A cloud-hosted student information system operated by a third-party vendor is compromised, exposing thousands of student records.

Potential Costs
- Notification expenses
- Legal defense costs
- Regulatory response
- Parent and student lawsuits

Cyber Coverage Typically Triggered
- Privacy Liability
- Dependent Service Provider Coverage
- Regulatory Defense Costs

10. AI-Enabled Deepfake Financial Fraud

Claim Scenario
A university finance officer participates in a video conference that appears to include the CFO. The video and voice are AI-generated. The officer is directed to make an urgent wire transfer which later proves fraudulent.

Potential Costs
- Financial loss
- Investigation expenses
- Funds recovery efforts

Cyber Coverage Typically Triggered

- Social Engineering Fraud
- Funds Transfer Fraud
- Crime Coverage

11. Distributed Denial of Service (DDoS) Attack During Enrollment

Claim Scenario

Attackers launch a DDoS attack against a university's admissions and enrollment systems during peak registration periods. Students are unable to register for classes or access online portals.

Potential Costs

- Emergency IT response
- Lost tuition revenue
- Extended staffing costs
- Vendor mitigation services

Cyber Coverage Typically Triggered

- Business Interruption
- Extra Expense Coverage
- Incident Response

12. Vendor-Dependent Business Interruption Claim

Claim Scenario

A university relies on a third-party cloud provider to host its Learning Management System (LMS), student portals, online testing platform, and course materials. The vendor suffers a ransomware attack that takes its environment offline for eight days.

Although the university's systems were never directly breached, students cannot access classes, submit assignments, take exams, or register for courses.

The university incurs significant expenses to implement temporary solutions, hire technology consultants, extend academic deadlines, and support affected students and faculty.

Potential Costs

- Lost revenue from delayed enrollment and registrations
- Additional IT consulting expenses
- Costs to deploy temporary learning platforms
- Overtime expenses for faculty and IT personnel
- Crisis communications and public relations expenses

Cyber Coverage Typically Triggered

- Dependent Business Interruption Coverage
- Contingent Business Interruption Coverage
- Extra Expense Coverage
- Incident Response Coverage

Why This Exposure Matters

Many educational institutions outsource critical functions to:

- Student Information System (SIS) providers
- Learning Management Systems (Canvas, Blackboard, Moodle, etc.)
- Payment processors
- Cloud storage providers
- Identity management providers
- Online testing platforms
- Managed IT service providers

An outage at one of these vendors can halt educational operations even when the institution itself remains secure. As a result, dependent business interruption coverage has become one of the most important components of a comprehensive cyber insurance program for educational institutions.

Executive Summary

The most significant cyber exposures facing educational institutions today typically fall into four categories:

Data Privacy Events

- Student records breaches
- Employee information breaches
- Health information exposures

Operational Disruption

- Ransomware
- DDoS attacks
- Dependent vendor outages
- Learning platform outages

Financial Fraud

- Business email compromise
- Social engineering
- Deepfake-enabled fraud
- Payroll diversion schemes

Third-Party Liability

- Parent, student, and employee lawsuits
- Regulatory investigations
- Contractual claims from vendors and research sponsors

Given the heavy reliance on cloud providers, student management systems, online learning platforms, and payment processors, educational institutions should ensure their cyber insurance programs include robust limits for incident response, privacy liability, cyber extortion, social engineering fraud, business interruption, and particularly dependent business interruption coverage, which can respond when a critical technology vendor suffers a cyber event that disrupts the institution's operations.

©2026 Innovation Growth Partners Specialty, LLC | igpspecialty.com