G2OPS
Smarter Intelligence.

Security Services for Higher Education

Prepare Now for to Reduce Impact from a Data Breach

Last year IBM and Ponemon Institute noted that the Education industry pays more per capita for a breach than 13 other industries due to their highly regulated nature. Breach costs for Education came in at $200, well over the $141 average cost[1].

Many higher education organizations remain exposed due to numerous compounding factors including costs, complexity, and the diversity of services they provide to Faculty, Staff, and Students. These factors present a unique challenge to Higher Education CIOs and CISOs.

G2OPS' deep understanding of higher education institutions, their technology infrastructures, regulatory requirements, and familiarity with resource challenges allow out team to partner with you in maturing your Cybersecurity Program while improving security posture.

[1] 2017 Cost of Data Breach Study. Ponemon Institute, LLC.

Security Services Features

- Define / Update Program Governance
- Validate / Implement Secure Architecture and Controls
- Assess Risk Profile
  - Develop Risk Register
  - Prioritize Mitigation Strategy
- Plan and Deliver Remediation Projects
- Maintain Compliance with Regulatory Requirements

Higher Education Security Challenges

1. Limited Resources
2. Awareness & Training
3. Device Management
4. Phishing/Malware/Ransomware
5. Compliance

***G2OPS** provides cybersecurity services to critical defense industry and commercial clients.*

Whether it is advisory level leadership with governance, project planning and execution, or simple security control implementation and configuration, let G2OPS' Higher Education expertise serve your institution's Cybersecurity Program. We focus on outcomes that provide actionable intelligence leading clients to improve security programs and reduce costly business interruption, brand damage, and the potential for burdensome financial loss.

Contact G2OPS today for a free Cybersecurity Consultation and learn how our expertise can benefit you.

✓ **Validate** Security Posture

✓ **Prioritize** Remediation Efforts

✓ **Satisfy** Compliance Requirements