Illuminate Education, Inc.
530 Technology Drive, Ste 100
Irvine, CA 92618
Phone: 949-656-3133
Fax: 909-266-1935

April 29, 2022

Security Incident Response Information

Incident Summary

On January 8, 2022, Illuminate Education became aware of suspicious activity in a set of isolated applications on our network.

- The incident was limited to specific databases.
- Only two platforms, IO Assessment and Data Driven Classroom, and one internal data transfer tool, IO Admin, were affected.
    - We do not store financial information or social security numbers on our systems so that type of information was not affected.
    - There is currently no evidence of actual or attempted misuse resulting from the incident.
- Law enforcement was notified immediately.

Steps were immediately taken to secure the affected applications and then we began restoration.

- Major system access and data has now been restored.

We also immediately engaged with external forensic investigators to determine the nature and scope of the activity.

- The investigation concluded on March 24, 2022.
- Illuminate has since been working to inform affected users and support them with any response requirements.

Unfortunately, cybersecurity threats exist across all industries. Public schools and their vendors have become increasingly common targets, with a dramatic rise since the onset of the COVID-19 pandemic[1].

- Nearly 1,400 unique incidents impacting public schools were reported in 2021[2].
- Many vendors, including Pearson, Finalsite, K12, Inc., and Zoom, have recently experienced similar incidents.

[1] https://www.k12six.org/the-report

[2] https://www.documentcloud.org/documents/20514564-pysa-ransomware-bc

Improved Security Measures

This was the first security incident of its kind that Illuminate and its acquired organizations have experienced over our more than 20 years in operation. Security is among our highest priorities, and additional steps beyond industry standard have been taken to earn the confidence of our clients and help prevent unauthorized access from happening in the future.

- Illuminate engaged with external advisors to conduct an extensive examination of our cloud environment.
    - Critical findings identified have already been resolved/addressed, and we continue to monitor and manage with both human audits and automated tooling.
- A comprehensive security audit and several enhancements were performed. Specific improvements were made, including though not limited to:
    - Continuous vulnerability monitoring, which includes:
        - Redundant detective and preventive controls for anomalous and malicious activity.
        - Third-party 24/7 monitoring on all AWS accounts and alerting to 24/7 on-call security team.
    - Clarifying and enforcing credential management policies including acceptable use, lifecycle management, and least privilege principles.
    - Enhancing our Secure Software Development Lifecycle policies.
    - Expanding and enforcing Single Sign-On (SSO) + Multi-Factor Authentication (MFA) capabilities.
    - Improving Business Continuity and Disaster Recovery (BCDR) readiness.
- We have expanded internal policies including:
    - AWS Identity and Access Management (IAM) Credential Policy with required semi-annual audits and validations.
    - Threat and Vulnerability Management (TVM) Policy and related processes for vulnerability scanning, patch management, and penetration testing.
- In line with new and updated policies, we have enhanced existing incident response procedures. For example:
    - Categorizing all findings from both static and dynamic tools used to monitor the security status of our environments as Critical, High, Medium, and Low.
        - Any Critical items found are entered into a structured Threat and Vulnerability Management system and these tickets are injected and prioritized in alignment with NIST 800-40 Rev 2 and Rev 3 standards.

Illuminate Education's commitment has always been to protect the privacy and data of students, families, and educators. While the unauthorized access we experienced in January was isolated and all data was restored, we take it and the commitments we make to our partners seriously. The steps outlined above highlight measures that go beyond standard practice to help prevent this from happening again.