STRATEGIC EDUCATION INC

StrategicEducation.com

2303 Dulles Station Blvd.,
6th floor, Herndon, VA
20171

SEI Cybersecurity Program Attestation

To Whom It May Concern:

SEI has a comprehensive Cybersecurity program covering all its universities and entities, including Capella University and Strayer University. The Cybersecurity program consists of 5 key pillars: Educate, Detect, Prevent, Respond and Remediate. SEI plans annually for investment in the training, tooling, and vendor partnerships to continually evolve and enhance the Cybersecurity program.

Educate

SEI publishes and maintains security awareness documentation, accessible by all employees, faculty and students. SEI conducts annual compliance training, comprised of relevant security training modules to cover existing and emerging threats to the organization and employees. In addition to readily available information and required training in 2021, SEI conducted a partner led Ransomware Tabletop exercise, where 40 key stakeholders across the organization participated and discussed the decision points throughout the theoretical exercise. SEI also conducts quarterly phishing campaigns to educate and verify the employee's ability to detect potential threats and keep the organizations systems, assets and customers data protected.

Detect

SEI has a dedicated, internal Information Security team responsible for acknowledgment, triage, and response of detected security events across services, infrastructure, and partners. The information security team evaluates emerging threats, trends, and published vulnerabilities, coordinating with appropriate teams on verification of any relevant threats and subsequent required remediations. SEI has implemented endpoint protection and detection software across all ender user assets, internal servers, and services, where applicable, feeding into a centralized data analytics platform. SEI has a Managed Security Services Provider (MSSP),

providing an extension of the Information Security team resulting in 24x7x365 security monitoring, triage, playbook response and escalation for security events.

Prevent

SEI has implemented and continually evolves a robust layered defense-indepth security pattern across end user devices, network, SaaS partners and infrastructure. SEI leverages leading industry solutions for endpoint protection, e-mail filtering, network intrusion and other protection solutions, ensuring a secure and resilient perimeter. SEI provides a robust Vendor Assessment process, providing in depth analysis and recommendations for SaaS products and partners. SEI deploys end user asset isolation technology, intended to halt malicious code execution and protecting the organization from further compromise.

Respond

SEI has implemented a robust, multi-layered approach to event detection, triage, incident identification and response. The multi-layered approach consists of First Response teams, Incident Commanders, a formal Cyber Security Incident Response Team (CSIRT), Leadership escalation protocols and partner engagement procedures. SEI's CSIRT consists of representatives across all major business functions, including individual University representation. SEI maintains robust communication protocols for all stakeholders and customers in the event of an incident or need for communication.

Remediate

SEI response teams maintain and continually improve incident response playbooks. A comprehensive ransomware specific playbook was developed and trained against in 2021 as a direct response to industry trends of escalating ransomware attacks and compromise. SEI employees, in partnership with the external MSSP and vendor partners, engage on any potential threat to the organization, triage, determine impact and execute remediations if required.

Sincerely,

STRATEGIC EDUCATION INC

StrategicEducation.com

2303 Dulles Station Blvd.,
6th floor, Herndon, VA
20171

Bernard Zavala
CISO