

Cybersecurity & Higher Education

Why Cybersecurity Now?

Cyberattack Risk



- ◆ There was a **31% increase** in reported cyberattacks from 2020 to 2021¹.
- ◆ **83% of organizations** studied experienced more than one data breach².
- ◆ **76% of data breaches** in the education sector were due to system intrusion, miscellaneous errors, and social engineering. **40%** involved malware and **30%** involved ransomware³.

Cost Savings



- ◆ **\$9.44 million** was the average total cost of a data breach in the US in 2021. For the education sector, the average total cost was **\$3.86 million**⁴.

Compliance



- ◆ Federal Trade Commission (FTC) has updated the Standards for Safeguarding Customer Information Rule ("**Safeguards Rule**") mandated under the Gramm-Leach-Bliley Act (GLBA)⁵.
- ◆ The Rule requires certain institutions to implement a comprehensive information security program, including nine elements outlined in 16 CFR Part 314, **by June 9, 2023**⁶.
- ◆ **Higher education institutions who accept federal student financial aid must comply** with GLBA⁷ and the Safeguards Rule. They are also encouraged to adopt **NIST SP 800-171 cybersecurity standards** by Federal Student Aid (FSA)⁸.
- ◆ In 2018 Federal Student Aid (FSA) began **auditing GLBA compliance**. "Colleges participating in the **FSA programs** are subject to the information security requirements established by the FTC for financial institutions." Noncompliance may result in **emergency actions, fines, limitations, suspensions, and terminations**⁹.



¹ https://www.accenture.com/_acnmedia/PDF-165/Accenture-State-Of-Cybersecurity-2021.pdf

² <https://www.ibm.com/reports/data-breach>

³ <https://www.verizon.com/business/resources/reports/2022/dbir/2022-data-breach-investigations-report-dbir.pdf>

⁴ <https://www.ibm.com/reports/data-breach>

⁵ <https://www.ftc.gov/news-events/news/press-releases/2021/10/ftc-strengthens-security-safeguards-consumer-financial-information-following-widespread-data>

⁶ <https://www.ftc.gov/news-events/news/press-releases/2022/11/ftc-extends-deadline-six-months-compliance-some-changes-financial-data-security-rule>

⁷ <https://library.educause.edu/topics/policy-and-law/gramm-leach-bliley-act-glb-act>

⁸ <https://fsapartners.ed.gov/knowledge-center/library/electronic-announcements/2023-02-09/updates-gramm-leach-bliley-act-cybersecurity-requirements#>

⁹ <https://fsapartners.ed.gov/knowledge-center/fsa-handbook/pdf/2021-2022>

Cybersecurity & Higher Education

We Can Help!

TCecure empowers clients to build and maintain effective cybersecurity programs.

Knowledge - Expert staff with industry-recognized certifications in project management and cybersecurity (PMP, CISSP, CIPP, CDPSE, CompTIA Security+, etc.).

Experience – 9+ years providing cybersecurity consulting, solutions, and education to federal and state government, academic, and commercial clients.

Value-Adds - Offering use of CyDeploy™, an automated tool that tests security updates to identify and prevent operational impact, and CySkills™, a customizable Learning Management System for on-demand training.

Plus, TCecure is a **Baltimore-based MBE/DBE/SBE** and **Qualified Maryland Cybersecurity Seller**.

TCecure can help your organization comply with the updated FTC Safeguards Rule.

Information Security Risk Assessment - We assess our client's current cybersecurity risk posture, then develop and implement mitigation strategies to close gaps. *TCecure supported 2 large contractors in implementing IT security necessary for federal agency authorization, and 10+ small contractors in meeting federal cybersecurity standards.*

Security-Related Policies and Procedures - We review existing and develop new documents, including Incident Response (IR) Plans, to accurately reflect our client's environment and help them achieve compliance. *TCecure has developed policies, procedures, and IR Plans for small and large federal contractors.*

Security Engineering and Software Assurance - We develop, test, and implement security and privacy controls to harden client IT environments and applications against attack vectors, using a variety of industry-recognized tools. *TCecure installed, configured, and upgraded multiple platforms, network solutions, and physical and virtual servers for the U.S. Air Force.*

Continuous Monitoring, Vulnerability Scanning, and Penetration Testing - We specialize in continuous monitoring, configuration management, and patch management to proactively prevent vulnerabilities. We conduct vulnerability scans and pen testing, then remediate findings. *TCecure has performed these services for large and small federal contractors, as well as two state agencies.*

Security Training and Education - We develop and deliver cybersecurity training and education in multiple modalities, tailored to our client's goals and the audience. *TCecure provided risk and security-related trainings to the U.S. Army, CMS, commercial businesses, Maryland colleges, and a local school system.*

Consulting and Advisory Services - We provide subject matter expertise to client leadership responsible for developing, implementing, supervising, and monitoring their cybersecurity programs. *TCecure helped stand up a security governance program at a Maryland college.*

Testimonial from a Maryland Community College: "TCecure's skills in Cybersecurity Business Analysis... Information Technology practices, Cybersecurity, and Risk Management Strategic Planning services are strong and comprehensive. TCecure is extremely knowledgeable of current events, the cybersecurity landscape, and governmental regulations. They worked well with people at all knowledge levels and communicated effectively."

Contact us today!

Tina Williams-Koroma,
Founder/CEO
tina.williams@tsecure.com
202-573-9344