TCecure
Our Eyes Where You Need Them

901 S Bond Street, Suite 203
Baltimore, MD 21231
202-573-9344
www.tcecure.com
info@tcecure.com

CAPABILITY STATEMENT

TCecure empowers clients to build and maintain effective cybersecurity programs.

Our Core Capabilities

√ Cybersecurity Program Management & Advisory Services

We provide subject matter expertise to leaders developing, implementing, and monitoring their cybersecurity programs. We identify and apply relevant regulatory and contract requirements, standards, and frameworks to support compliance (e.g., FISMA, HIPAA, NIST CSF, NIST SP 800-53). TCecure developed and implemented security governance and risk management programs for federal contractors and a college with a medical education program. We also developed written programs, policies, and procedures, including Incident Response Plans and testing.

√ Security Risk Assessment & Mitigation

We assess our client's current cybersecurity risk posture using industry best practices, frameworks, and standards. We then develop and implement mitigation strategies to close gaps, reducing vulnerabilities and exposure to risks. TCecure supported two federal contractors in obtaining authorization to operate (ATO). We have performed assessment and mitigation services for federal and state agencies including a state mental health agency, agency contractors, and commercial clients including a medical equipment company.

√ Security Engineering & Software Assurance

We develop, test, and implement security and privacy controls to harden client IT environments and applications against attack vectors. We specialize in continuous monitoring, configuration management, and patch management solutions to proactively prevent vulnerabilities. TCecure has provided security-focused network and system administration support to a federal agency, including installation, configuration, and upgrading of multiple platforms, network solutions, and physical and virtual servers. We also performed remediation activities for a non-profit in the health and human services sector.

√ Security Training & Education

We develop and deliver cybersecurity training and education tailored to our client's goals, desired modalities, and participants/audience. TCecure has provided training courses to federal agencies including CMS, as well as commercial businesses and colleges. We managed training and certification requirements for a federal agency, including credential maintenance and personnel compliance.

Healthcare Applications

- Secure PHI and PII by applying industry best practices
- Take a holistic approach to secure IT, IOT, and OT systems and integration
- Determine cyber risks of business partnerships & acquisitions
- Manage security patches to minimize delays, operational impacts, & downtime
- Provide role-based training to end users and IT staff responsible for security tasks
- Prepare & plan for cybersecurity incidents

... AND MORE!

Why TCecure?

Knowledge – TCecure's expert staff has decades of experience and industry-recognized certifications in project management and cybersecurity (PMP, CISSP, CIPP, CDPSE, CompTIA Security+, etc.).

Experience – For over 9 years, TCecure has provided cybersecurity consulting, solutions, and education to federal and state government agencies, large and small businesses, and academic institutions.

Value Adds – TCecure offers CyDeploy, an automated tool that tests security updates to identify/prevent operational impact, and CySkills, a customizable Learning Management System for on-demand training.

Contact:

Melanie Brennan, President
443-340-5152
melanie.brennan@tcecure.com

Tina Williams-Koroma,
Founder/CEO
tina.williams@tcecure.com

Happy Customers –

"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 the current events, the cybersecurity landscape, and governmental regulations. They worked well with people at all knowledge levels and communicated effectively."

"TCecure helped [us] save money... They supplied knowledgeable and experienced engineers [who] were proactive in identifying and resolving possible issues… All due dates were met or exceeded… [They] maintained excellent communication."

"TCecure has been a trusted partner on this program for more than five (5) years… They are communicative, responsive, and their personnel are highly valued by the Government customer. They meet deadlines, and correct any issues identified."

Why Now?

Increasing Risk. In 2022, the healthcare sector experienced a 60% year-over-year increase in cyberattacks, with more ransomware attacks than any other sector[1]. 594 data breaches exposed or disclosed nearly 38 million individuals' records that year[2].

Patient Harm. Ransomware attacks targeting healthcare organizations doubled in the last five years, disrupting care and exposing the PHI of nearly 42 million patients[3]. Such attacks are linked to worsening patient outcomes and increased mortality rates by surveyed Healthcare Delivery Organizations[4].

Increasing Cost. The average cost of a healthcare data breach increased 42% to $10.1 million in 2022, the highest cost for any industry for 12 consecutive years. 33% of this cost is from lost business[5]. 72% of surveyed U.S. adults read online reviews when choosing a healthcare provider. Ratings and reviews were the third most important decision factor[6].

Compliance. The HIPAA Security Rule requires administrative, technical, and physical safeguards to protect e-PHI[7]. The White House plans to implement additional minimum cybersecurity guidelines.[8]

---

[1] www.hipaajournal.com/healthcare-sees-60-yoy-increase-in-cyberattacks/
[2] www.hipaajournal.com/october-2022-healthcare-data-breach-report/
[3] https://jamanetwork.com/journals/jama-health-forum/fullarticle/2799961
[4] www.censinet.com/ponemon-report-covid-impact-ransomware
[5] www.ibm.com/reports/data-breach
[6] https://go.reputation.com/hubfs/Downloadable%20Assets/five-healthcare-trends-2022.pdf
[7] www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html
[8] www.washingtonpost.com/washington-post-live/2022/10/13/transcript-securing-cyberspace/