Texas Businesses Are Exposed, Even With Backups and Antivirus in Place

East Texas technology and cybersecurity provider warns that antivirus, backups, and standard IT support only represent part of a complete cybersecurity program.

TruePoint Systems helps Texas businesses understand where backups, antivirus, and standard IT support may fall short of a complete cybersecurity program.

LONGVIEW, TX, UNITED STATES, July 9, 2026 /EINPresswire.com/ -- A single data breach can be the difference between a Texas business staying protected and ending up in court. As Texas businesses evaluate the implications of Texas Cybersecurity Safe Harbor protections, many owners begin with a common assumption: if they already have a managed IT provider, their cybersecurity responsibilities are covered. According to TruePoint Systems, that assumption may leave important questions unanswered.

Traditional managed IT services often include help desk support, software updates, backups, network management, and endpoint protection. While these services play an important role in daily business operations, they may represent only part of what qualifying organizations need to establish, maintain, and document a comprehensive cybersecurity program. “Business owners often believe that hiring an MSP means every aspect of cybersecurity has been addressed,” said Stepp Sydnor, CEO of TruePoint Systems. “The reality is that managed service agreements vary considerably. Businesses need to understand whether someone is also overseeing policies, training, risk management, documentation, and the ongoing cybersecurity program.”

> The harder question is whether the business can demonstrate that it had a complete and actively maintained cybersecurity program before an incident occurred.”
>
> *Clint Boggio, CTO of TruePoint Systems*

Texas Business & Commerce Code Chapter 542 establishes a cybersecurity Safe Harbor

framework for qualifying Texas businesses with fewer than 250 employees. In an action arising from a breach of system security, the law may prohibit the recovery of exemplary damages if the business can demonstrate that it had implemented and maintained an appropriate cybersecurity program at the time of the breach.

According to TruePoint Systems, that distinction is important.

Cybersecurity tools such as antivirus software, firewalls, multifactor authentication, monitoring platforms, and data backups can be important components of a cybersecurity strategy. However, these tools alone do not constitute a comprehensive cybersecurity program.

A broader cybersecurity program may include administrative, technical, and physical safeguards, as well as documented policies and procedures, employee cybersecurity awareness training, risk assessments, access controls, incident response planning, ongoing review, and alignment with a recognized cybersecurity framework.

“A firewall can be configured. Backups can be monitored. Antivirus can be installed,” said Clint Boggio, CTO of TruePoint Systems. “The harder question is whether the business can demonstrate that it had a complete and actively maintained cybersecurity program before an incident occurred.”

TruePoint Systems provides more than traditional technology support by bringing managed IT services, cybersecurity, compliance support, risk management, and strategic technology guidance together under one accountable provider.
The company’s services include managed IT and infrastructure support, network and endpoint security, managed detection and response, threat monitoring, employee security awareness training, backup and disaster recovery planning, communications infrastructure, compliance support, and strategic technology advisory services.

This integrated approach is designed to help organizations identify potential gaps that may otherwise exist among separate technology vendors, security tools, internal departments, compliance initiatives, and business leadership responsibilities.

“Cybersecurity today impacts every area of an organization,” Sydnor said. “It affects operations, leadership, employees, vendors, customers, business continuity, and overall risk. Organizations need visibility into the entire cybersecurity picture, not just the technology tools being used.”

TruePoint Systems does not provide legal advice or determine whether a business qualifies for protections under Texas law. Businesses should consult qualified legal counsel regarding Safe Harbor interpretation, legal requirements, and eligibility considerations.

TruePoint’s role is to help organizations evaluate their cybersecurity posture, identify potential gaps, strengthen safeguards, and improve the documentation and practices that support

cybersecurity readiness.

Business leaders evaluating their current technology and cybersecurity environment may benefit from asking:

- Is our cybersecurity program documented?
- Are responsibilities clearly defined between our company and our providers?
- Are employees receiving cybersecurity awareness training?
- Do we have an incident response plan?
- Are safeguards reviewed and updated regularly?
- Are our practices aligned with a recognized cybersecurity framework?
- Could we demonstrate what was implemented and maintained before a breach occurred?

TruePoint Systems offers a Safe Harbor Readiness Review designed to help Texas businesses better understand their current cybersecurity posture and identify potential next steps toward a stronger, better-documented cybersecurity program.
For more information or to schedule a Safe Harbor Readiness Review, visit the TruePoint Systems website.

About TruePoint Systems

TruePoint Systems provides managed IT services, cybersecurity solutions, communications infrastructure, cloud services, and strategic technology support for organizations across Texas. By bringing technology operations, cybersecurity, and business strategy together under one accountable provider, TruePoint helps businesses improve security, reduce risk, and support operational success.

Stepp Sydnor
TruePoint Systems
email us here
Visit us on social media:
LinkedIn
Facebook