SKINNER
TECHNOLOGY GROUP

Emerging Technologies & Cyber Risk in Healthcare

Mike Skinner

08.28.2025

Skinner Technology Group

The global healthcare data storage market size was 5.4 billion USD in 2024.

SKINNER
TECHNOLOGY GROUP

Emerging Technologies

SKINNER
TECHNOLOGY GROUP

Artificial Intelligence, Generative AI

5G Network

Internet of Things (IoT)

Cloud Computing

The AI healthcare market is projected to reach $868 billion by 2030.

SKINNER
TECHNOLOGY GROUP

How is AI being used?

- As of today, AI is leveraged for speed and increased accuracy.
- Diagnosing Patients: Analyzing X-rays, MRIs, and CT scans, predicting risk of cancer, and recognizing skin cancer
- Transcribing Medical Documents: Automatic speech recognition technology can convert spoken language into written text, efficiently and accurately documenting medical information
- Administrative Tasks: Admission procedures, appointment scheduling, customer service responses, licensure verification, etc.

How is AI being used?

SKINNER
TECHNOLOGY GROUP

- Financial uses: billing and collections, claims management, insurance eligibility verification, revenue cycle management
- Operational tasks: facilities management, inventory management, materials management

Robotic Process Automation

What risks does AI bring?

SKINNER
TECHNOLOGY GROUP

- Ethical concerns and data privacy issues: With more & more data being collected and analyzed, there is an increased concern over the use of private and personal data used to train AI algorithms. Furthermore, healthcare entities and their third-party vendors are particularly vulnerable to data breaches and ransomware attacks.
- Possibility of bias in underlying algorithms: AI algorithms may be skewed due to a lack of data for women and minorities.
- Trust issues: **60%** of Americans would be uncomfortable with their provider relying on AI, which could lead to worse patient-provider relationships.

The healthcare IoT market is expected to show an annual growth rate (CAGR 2025-2029) of 9.56%, leading to a market volume of $134.43 billion by 2029.

SKINNER
TECHNOLOGY GROUP

IoT: Uses and Benefits

IoT (or Internet of Medical Things (“IoMT”))in healthcare spans across patient services and internal operations. Examples include smart infusion pumps, wearable health monitors, remote patient monitoring tools, connected imaging systems, and even hospital HVAC systems.

Benefits:

- Enhanced patient care
- Improved operational efficiency and care cost reduction
- Medical care accessibility through telehealth
- Data driven insights to aid decisions

IoT Related Risks

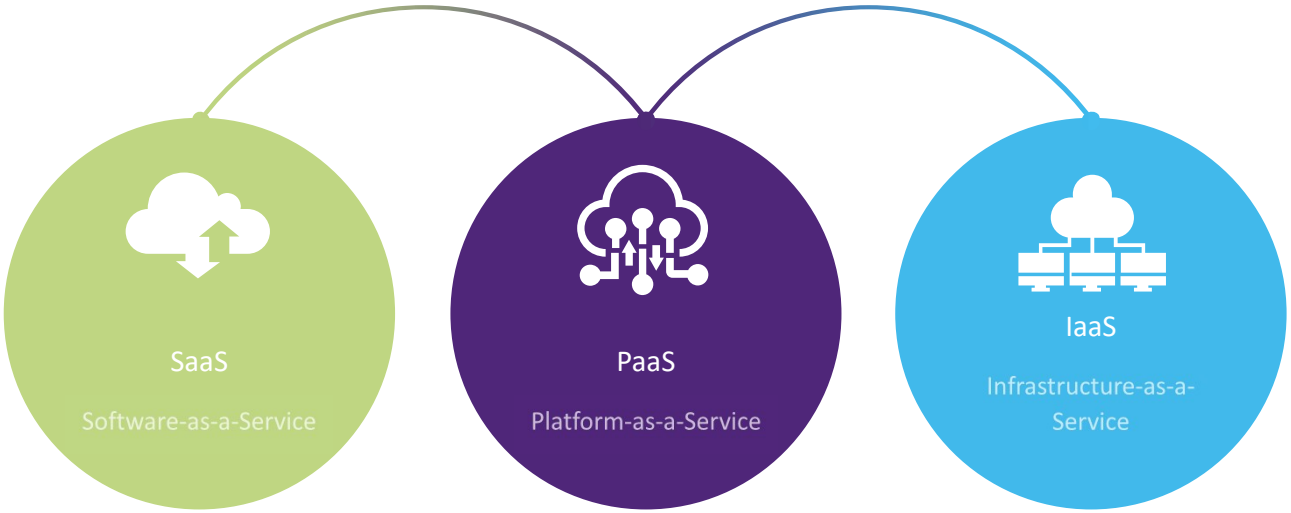
SKINNER
TECHNOLOGY GROUP

- More devices = more potential breach points
- Lack of oversight
- Unencrypted or inadequately encrypted data may be vulnerable to interceptions, allowing cybercriminals to eavesdrop on data transmissions
- Cloud services and on-premises servers may not have sufficient security measures

70 - 80% of hospitals and health systems have adopted cloud computing services.

SKINNER
TECHNOLOGY GROUP

Common Cloud Service Models in Healthcare



Strengths of Cloud Computing

- Accelerate clinical analyses and care processes
- Automates data processing and scalability
- Makes patient data easier to share and access
- Reduces network equipment on-site
- Reduces risk of data loss

Cloud Computing Risks

- The healthcare organizations struggle to with the skill gap for cloud security deployment and management.
- Applications and resources hosted in the cloud are reliant on network connectivity with downtime heavily impacting operations.
- Calls for strong vendor management practices and understanding of shared responsibility (For example, user access controls).

AI Attacks

SKINNER
TECHNOLOGY GROUP

DMCA Copyright Infringement Notice

Lea Davis | Citi Legal Services <lea@cl-service.net>
To Skinner Technology Group

Reply | Reply All | Forward

Tue 10/8/2024 6:05 PM

You replied to this message on 10/8/2024 6:11 PM.
We could not verify the identity of the sender. Click here to learn more.
We removed extra line breaks from this message.

Dear owner of https://linklock.titanhq.com/analyse?url=https%3A%2F%2Fskinnertechgroup.com%2Fa-double-edged-sword-understanding-ai-in-cybersecurity%2F&data=eJxsym9KwzAUAPDTpB-EV16ztyQFIw60CMIm_jlAmjy7sDYdSars9l7A7z9vQ4e6R-zAEfVARivox_EbNKFWNGraK9cEe9cs9r5DZfaq3ynTdopU22lpSBqNiEY-Pj1_vH6e3uDl9H78Oh4emmJndoLQz1A4_0TPbeLaZLvECwvCcokpca7sz1Net2vr16XZ7LnWaxG7g5CDkMN_SMjBQVi3cWbgMHGA8rvmAFsKnEt1KcQ0gYsQE_jbyLmw33KsNyGHvwAAAP__jKFMTw%%,

I represent the Intellectual Property division for claudeai.wiki. We have identified an image belonging to our client on your website.

Image Details: https://linklock.titanhq.com/analyse?url=https%3A%2F%2Fi.imgur.com%2FpJvUtY8.png&data=eJwUyUFPwyAUAOBfAwcTyIO9PWgixiXaGE02o-7gsWXYka2MAO3vNzt_3p0UmA5AiQGxE2gNiW4c_4RBMISjwS0N_OQe-OweFZDdUrchKxUhSWW0RW0NAFj9_PL6_fFz-BRvh6_9cb974tVdw8AQ_FXUUNbog0yh8eLmeAkMoV5iSqG04M9TuS1Z-tvMF3duLVe22THdM91HGedpKXdjus_v67H9WpnT9B8AAP__QsU2vA%%
Location of Usage: https://linklock.titanhq.com/analyse?url=https%3A%2F%2Fskinnertechgroup.com%2Fa-double-edged-sword-understanding-ai-in-cybersecurity%2F&data=eJxsym9KwzAUAPDTpB-EV16ztyQFIw60CMIm_jlAmjy7sDYdSars9l7A7z9vQ4e6R-zAEfVARivox_EbNKFWNGraK9cEe9cs9r5DZfaq3ynTdopU22lpSBqNiEY-Pj1_vH6e3uDl9H78Oh4emmJndoLQz1A4_0TPbeLaZLvECwvCcokpca7sz1Net2vr16XZ7LnWaxG7g5CDkMN_SMjBQVi3cWbgMHGA8rvmAFsKnEt1KcQ0gYsQE_jbyLmw33KsNyGHvwAAAP__jKFMTw%%

We require that you credit claudeai.wiki for this image. Please add a direct and clickable hyperlink to https://linklock.titanhq.com/analyse?url=https%3A%2F%2Fclaudeai.wiki%2F&data=eJwEwP1KBCEQAPCn0T8CZfTmRhcyOqglCO6ijwdw3amT_bhF3Xr9fimMBlwHYFRE7BR6R6obhm_lEBzh4PBIUY7hTi7h3gD5I3UH8toQkjbOerTeAYC3j0_PH6-flzf1cnk_f51PD7KGmaNASLOqXH5zYr1ykyUseWKBUKe8rlwap-tPue2bTrdF7uHa2lbF4SRsL2yf5riPHLP-y1MWtv8PAAD__2aRM7E% either beneath the image or in the footer of the page. This must be completed within the next five business days.

Please understand the seriousness of this request. Simply removing the image will not suffice. If you do not comply within the given timeframe, we will have to start legal proceedings under case No. 84132, following the DMCA Section 512(c) guidelines.

For historical image usage, you can check the Wayback Machine at https://linklock.titanhq.com/analyse?url=https%3A%2F%2Fweb.archive.org&data=eJwEwO9qwyAQAPCn0Q8D5bTX08AcK2xlMGjH_jyA2lsjbZKiNnv9_XI4GXADgFERcVDoHakhpV_lEBxhcrilKE_hQU7h0QD5LQ0b8toQkjbOerTeAYC3zy-vX-_fxw_1dvw8_Bx2T7KFK0eBkK-qcV1LZj1zlzVM5cICoV3KPHPtnMdzXe43nZdJ3sPY-62JzU7YvbD7P0461jyWlfVSz_8BAAD__zI-M74%.

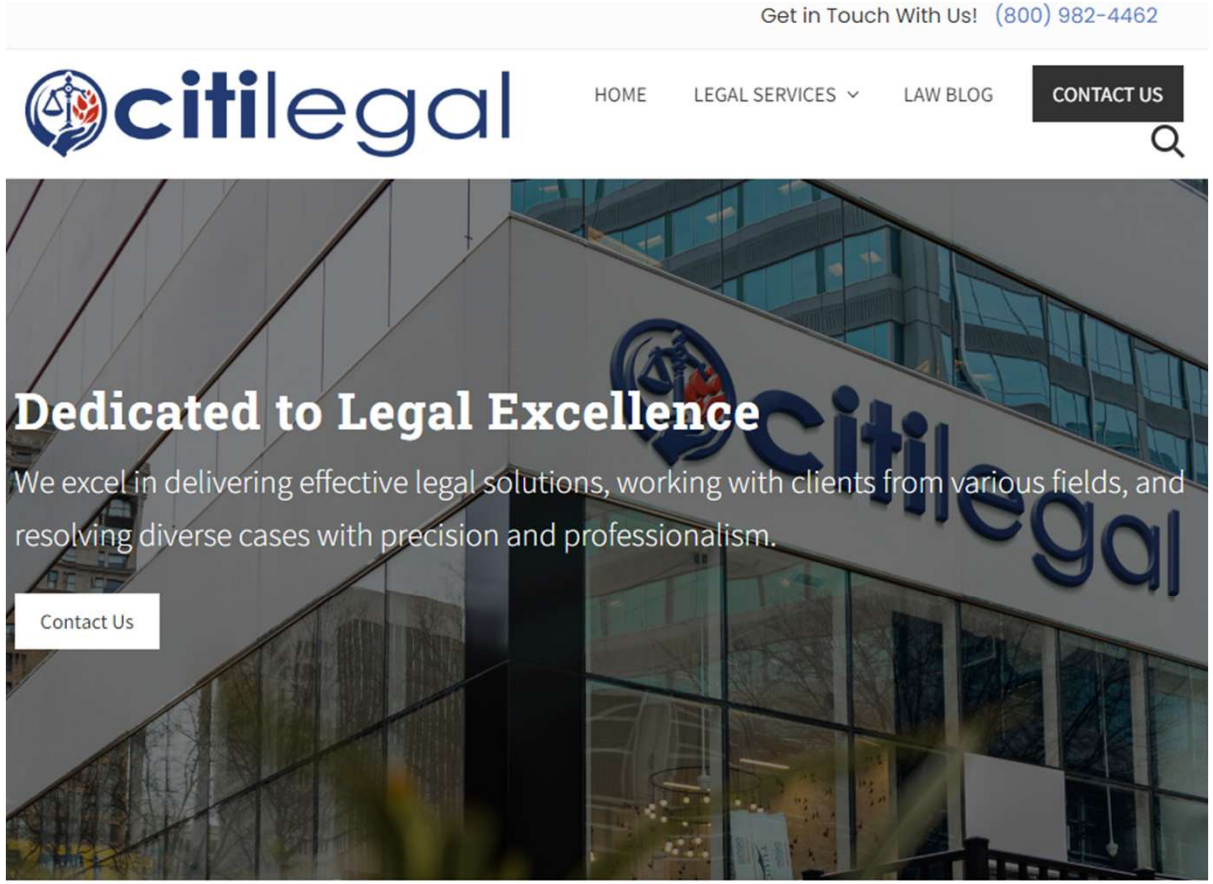
This is an official notice. We value your prompt response and cooperation. Please correspond in English.

Regards

Lea Davis
Trademark Attorney

Citi Legal Services
1 Beacon St 12th floor
Boston, MA 02108

lea@cl-service.net
www.cl-service.net



Welcome to Citi Legal

Our team of skilled attorneys is dedicated to delivering top-tier legal representation. Whether you're facing a contract dispute, personal injury claim, or any other legal matter, we're here to help. Reach out to us today to schedule a consultation with one of our experienced attorneys.

Read More

Read More

Read More

Luke Worthington

Copyright and Patent Law

Read More

Mary Sinclair

Property Expert

Read More

Sally Beaumont

Copyright Compliance / Business Law

Read More

Rob Anderson

Intellectual Property / Corporate Governance

Read More

Greg Kensington

Property Arbitration

Read More

Lea Davis

Copyright Infringement / Criminal Litigation

Read More

Managing Risk while Embracing Technology

SKINNER
TECHNOLOGY GROUP

Foster Awareness & Training

SKINNER
TECHNOLOGY GROUP

- Staff members — from medical professionals to administrative personnel — are often the first line of defense against cybersecurity threats.
- Healthcare organizations can reduce the risk of breaches by fostering a culture of active participation and responsibility in staff.
- Human factors affect approximately 74% of breaches including errors, social engineering, and misuse, highlighting the need for comprehensive employee training and awareness programs.

Cybersecurity

SKINNER
TECHNOLOGY GROUP

- Security = Key to maintaining patient’s trust
- Implement cybersecurity measures such as Zero-trust
- Build hardened infrastructures that protect against both legacy and evolving vulnerabilities
- Implementing strict access controls, network segmentation, and data protection techniques to protect patients' most sensitive information

Internal Audit Strategies

- Risk assessment and identification of technology-specific vulnerabilities.
- Evaluation of controls and security measures implemented for emerging technologies.
- Continuous monitoring of technology-related risks and threat landscape.
- Collaboration with IT teams, management, and external auditors to assess risks comprehensively.

Third-Party Risk Management

SKINNER TECHNOLOGY GROUP

5 keys strategies when managing 3rd party risks:

1. Due diligence before partnering with an emerging tech organization
2. Review insurance coverage – Is it still sufficient?
3. Assess your organization's responsibilities and monitor control performance
4. Regular assessments of security practices for alignment with organizational standards
5. Review contracts for compliance with new and evolving privacy laws

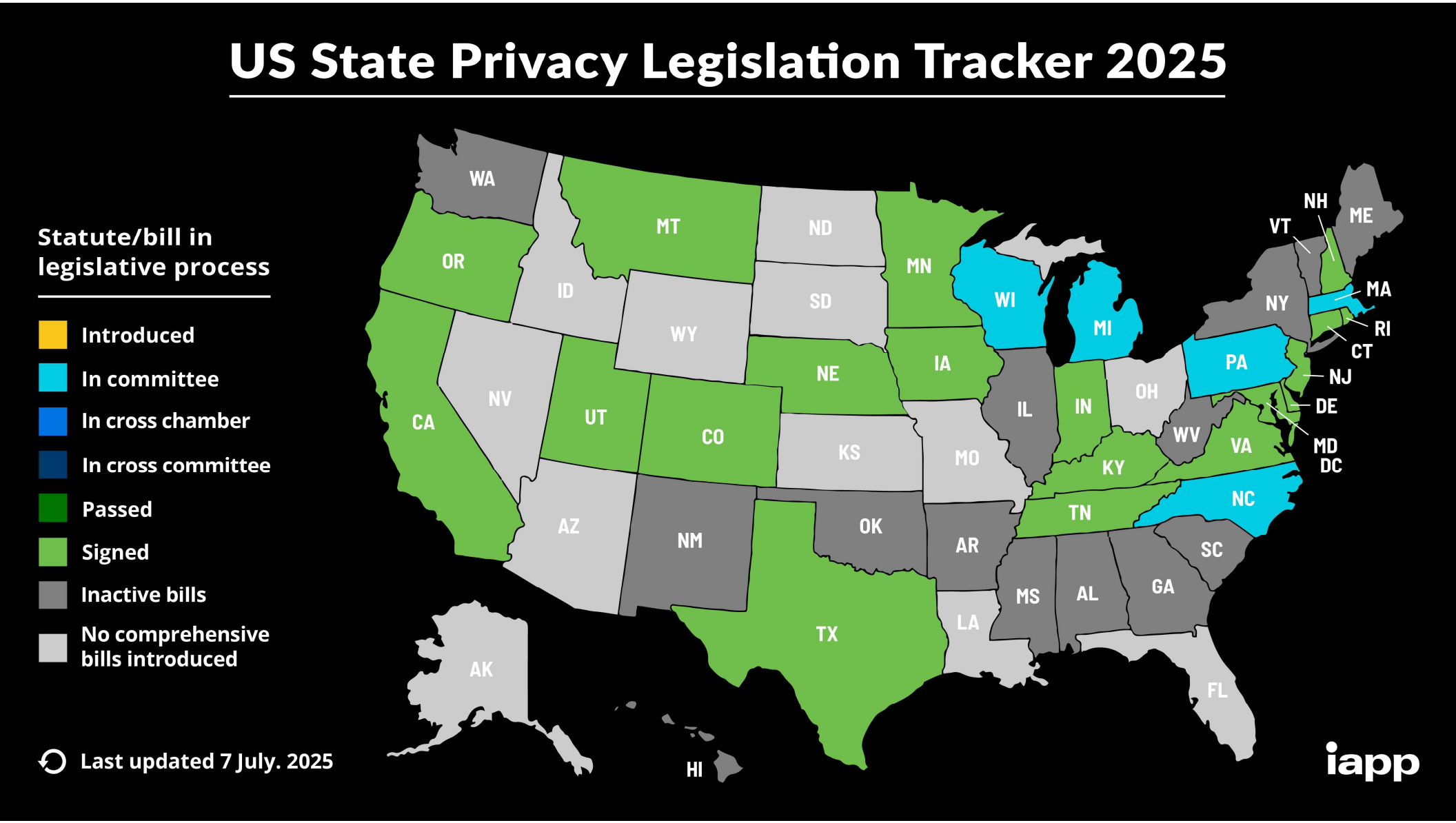
Regulatory & Compliance Considerations

SKINNER
TECHNOLOGY GROUP

Broader data privacy regulations will continue to evolve as policies are adopted in US states and internationally

- These regulations impact the data that is processed, stored, and analyzed by emerging technologies.
- Currently, 10 states have AI-related regulations as part of their larger consumer privacy laws; however, only a handful of states have proposed legislation specific to the privacy of data or the use of AI in healthcare.
- Updates to the HIPAA Security & Privacy Rules

US State Privacy Legislation Tracker 2025



HIPAA Security Rule Proposed Changes 2025

- Removal of “addressable” standards which would mean implementation specifications are mandatory
- Mandatory encryption for all ePHI at rest and in transit
- Require MFA as a security measure to enhance ePHI protection
- Regularly scheduled security assessments would be required
- Detailed guidelines and expectations for security incident response
- Alignment with NIST cybersecurity best practices
- Individual increased rights over their ePHI

Cybersecurity Safe Harbor

- Texas becomes 5th state to implement a cybersecurity safe harbor and the sixth to meaningfully define “reasonable cybersecurity” in statute
- TX Senate Bill 2610 signed in to law
  - Incentivizes businesses to adopt strong cybersecurity programs by offering protection from exemplary (punitive) damages in the event of a data breach, provided they meet specific cybersecurity criteria
- Tiered approach to cyber requirements based on company size
  - < 20 EEs
  - 20-99 EEs
  - 100-249 EEs
- Ohio, Utah, Connecticut and Nevada

Thank you!

Mike Skinner, CPA, CITP
Principal Consultant
mike@skinnertechgroup.com

SKINNER
TECHNOLOGY GROUP