Cybersecurity for Nonprofits

May 2026

Larson
CERTIFIED PUBLIC ACCOUNTANTS

Cameron Hodson

CPA, CISA | Senior Manager

Aflac Social Engineering Attack

Help-Desk Staff Targeted

Attackers impersonated support teams to trick Aflac's help-desk staff, leading to unauthorized access.

Rapid Breach Containment

Aflac detected and contained the breach within hours, minimizing potential impact and further exposure.

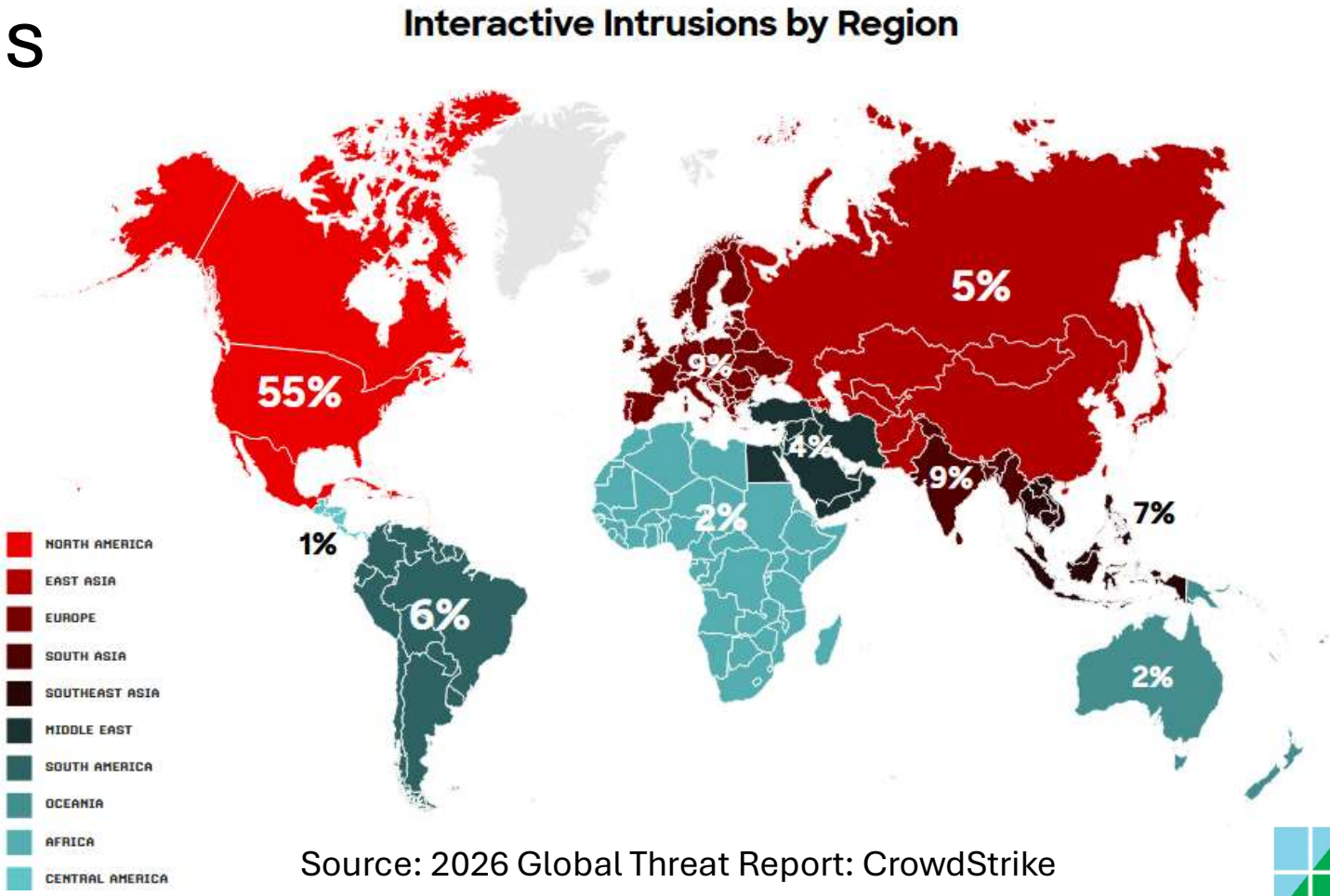
Personal Data Exposure

The attack exposed personal and health information of about 22.65 million people, including Social Security numbers.

Aftermath and Support

Aflac provided credit monitoring and faced regulatory scrutiny, although ransomware was not involved in the incident.

Trends



Source: 2026 Global Threat Report: CrowdStrike

Larson
CERTIFIED PUBLIC ACCOUNTANTS

Agenda

- Today's Top Threats
  - Business E-mail Compromise (BEC)
  - Ransomware
  - Social Engineering
  - Generative AI Scams
  - 3rd Party Risk
- Regulation
- Future Threats
- Quiz

Larson
CERTIFIED PUBLIC ACCOUNTANTS

Social Engineering

Larson
CERTIFIED PUBLIC ACCOUNTANTS

Understanding Social Engineering

Manipulation for Information

Social engineering relies on manipulating people to gain access to confidential information or systems. It targets human behavior rather than technical flaws.

Psychological Tactics Used

Attackers use methods like impersonation, phishing, and pretexting to trick individuals into revealing sensitive data or credentials.

Importance of Awareness

Training and awareness are crucial for recognizing and preventing social engineering threats in both personal and organizational environments.

Social Engineering: Phishing

Social Engineering Prevention

TRAINING

MULTI-FACTOR AUTHENTICATION (MFA)

POLICIES

Larson
CERTIFIED PUBLIC ACCOUNTANTS


Business E-mail
Compromise (BEC)
Larson
CERTIFIED PUBLIC ACCOUNTANTS

Business E-mail Compromise

Larson
CERTIFIED PUBLIC ACCOUNTANTS

BEC Prevention

TRAINING

MULTI-FACTOR AUTHENTICATION

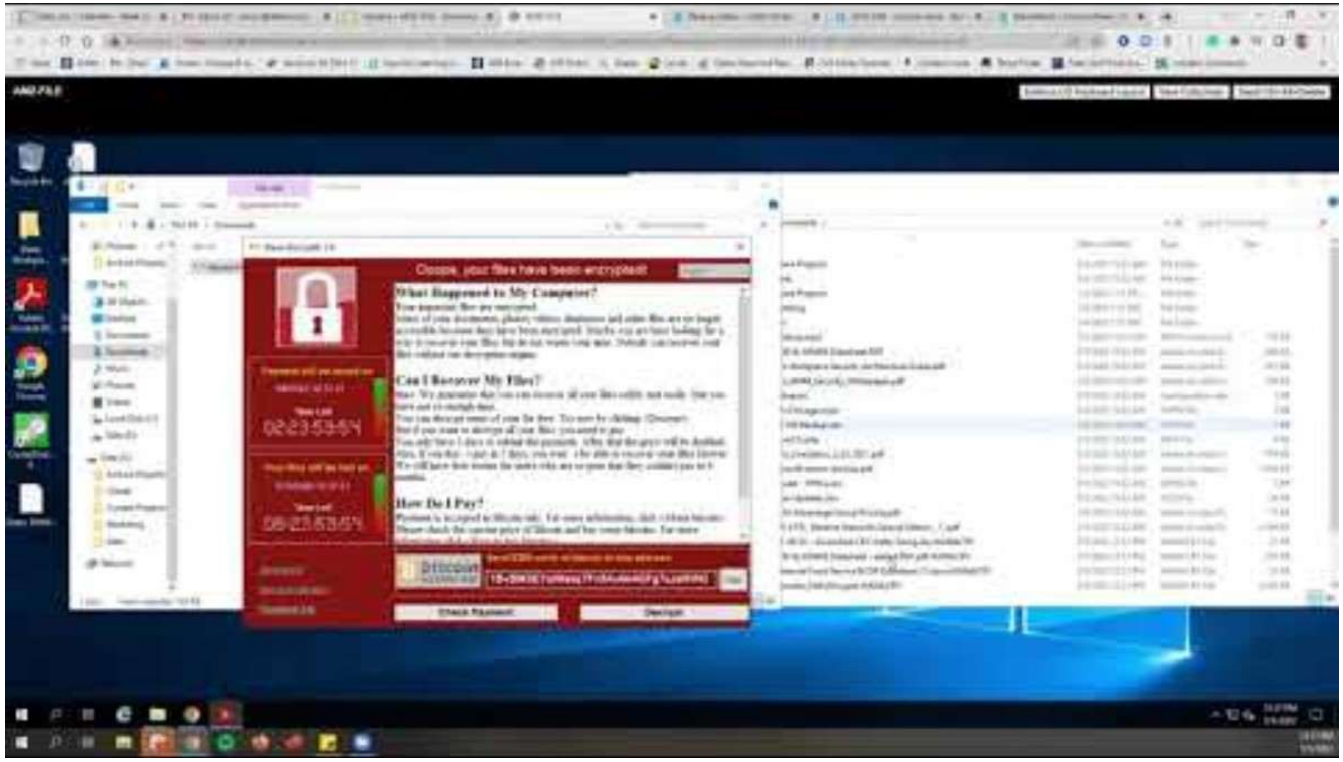
MONITORING (EXTERNAL VS. INTERNAL)

VENDOR MANAGEMENT

Larson
CERTIFIED PUBLIC ACCOUNTANTS


Ransomware
Larson
CERTIFIED PUBLIC ACCOUNTANTS

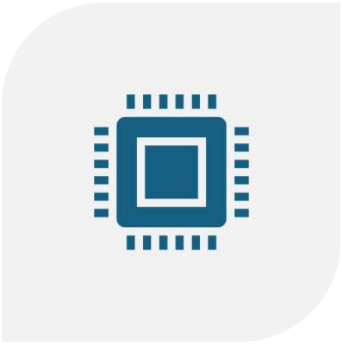
Ransomware



Larson
CERTIFIED PUBLIC ACCOUNTANTS

Ransomware Prevention

TRAINING



ENDPOINT PROTECTION SYSTEMS (PATCHES, ANTI-VIRUS, ETC)

BACK-UPS

Larson
CERTIFIED PUBLIC ACCOUNTANTS

Generative AI Scams

Larson
CERTIFIED PUBLIC ACCOUNTANTS

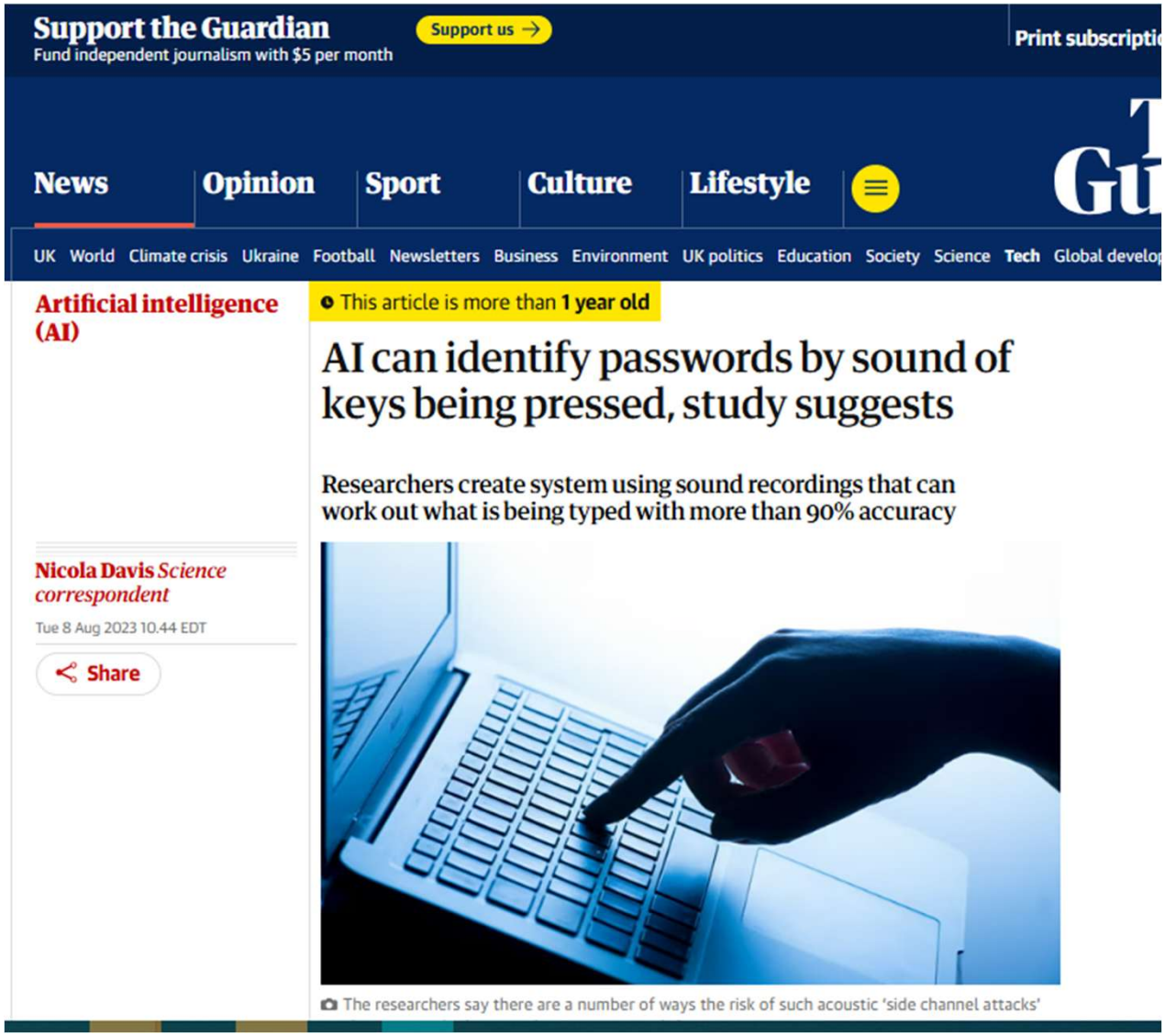
Generative AI Scams

Larson
CERTIFIED PUBLIC ACCOUNTANTS

Generative AI Scams

Larson
CERTIFIED PUBLIC ACCOUNTANTS

Generative AI Scams



Larson
CERTIFIED PUBLIC ACCOUNTANTS

Generative AI Scams Preventions

- Training
- Web Content Management
- Policies for Work Environment and Gateways
- Password Managers coupled with MFA

3rd Party Risk

3rd Party Risk

Donor

Nonprofit

Larson
CERTIFIED PUBLIC ACCOUNTANTS

Understanding Vendor Risks

Trusted Vendors Have More Access

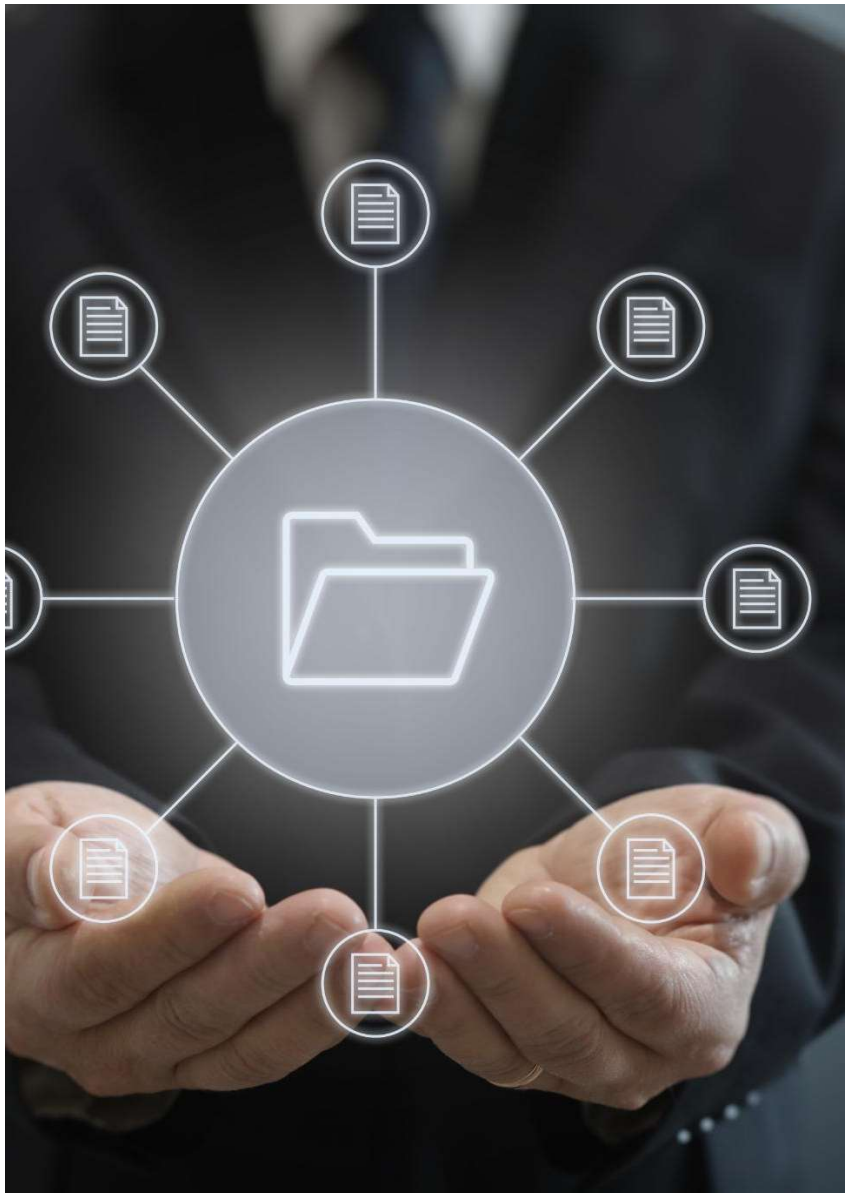
Vendor employees or systems are already “trusted” and, if compromised, have higher levels of access or are more likely to succeed with phishing attacks.

Cybersecurity Threats

Sensitive data can be exposed or compromised through third-party vendors

Operational Disruptions

Vendor process failures may disrupt business continuity, impacting operations and causing delays or losses.

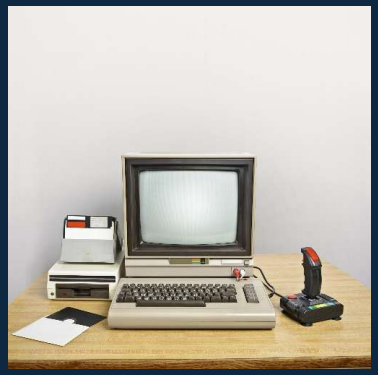


3rd Party Risk Prevention

Larson
CERTIFIED PUBLIC ACCOUNTANTS

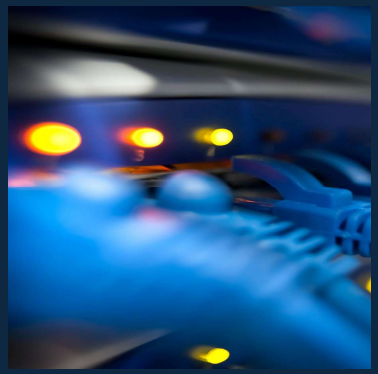

Other Noteworthy Threats
Larson
CERTIFIED PUBLIC ACCOUNTANTS

Other Risks



Legacy Technology Vulnerabilities

Outdated software and unsupported hardware increase risk of cyberattacks, making IT environments susceptible to exploitation.



Shadow IT Threats

Unauthorized applications and devices bypass security protocols, creating unseen risks and undermining IT defenses.

Preventing Legacy Tech & Shadow IT Risks

Decommission Legacy Systems

Regular updates and decommissioning old technology reduce vulnerabilities and strengthen organizational cyber security posture.

Control Shadow IT Activities

Strict IT policies and user education help monitor and control unauthorized technology use, reducing hidden risks.

Centralized Security Monitoring

Employ centralized security systems and access controls to detect unauthorized applications and ensure compliance across all assets.

Prevention Heatmap

Prevention Technique	BEC	Ransomware	Social Engineering	GenAI Scams	3rd Party Risk
Policies (Security / IT / Acceptable Use)	🟩	🟩	🟩	🟩	🟩
Training / Awareness	🟩	🟩	🟩	🟩	🟩
Multi-Factor Authentication (MFA), Passkeys	🟩	🟩	🟩	🟩	🟩
Vendor Management	🟩	⬜	🟩	⬜	🟩
Monitoring (Internal vs External)	🟩	🟩	⬜	⬜	🟩
Endpoint Protection (Patching, AV)	🟩	🟩	⬜	⬜	🟩
Backups	⬜	🟩	⬜	⬜	⬜
Web Content Management	⬜	⬜	🟩	🟩	⬜
Annual Information Inventory	⬜	⬜	⬜	⬜	🟩

Other Recommended Controls

Larson
CERTIFIED PUBLIC ACCOUNTANTS

Other Recommended Controls

- Policies
- Monitoring: automated + manual
- Tabletop exercises
- Risk Assessments/NIST
- Vendor Management

Larson
CERTIFIED PUBLIC ACCOUNTANTS

Essential Organizational Policies

1. Acceptable Use Policy
2. Privacy Policy
3. Password Policy
4. Disposal and Destruction Policy
5. Storage and Retention Policy
6. Incident Response Policy
7. Classification Policy
8. Human Resource Policy
9. Change Management Policy (include hardening)
10. Firewall Policy
11. AI Governance Policy

Larson
CERTIFIED PUBLIC ACCOUNTANTS

Regulatory Trends

Larson
CERTIFIED PUBLIC ACCOUNTANTS

Recent Regulatory Change Examples

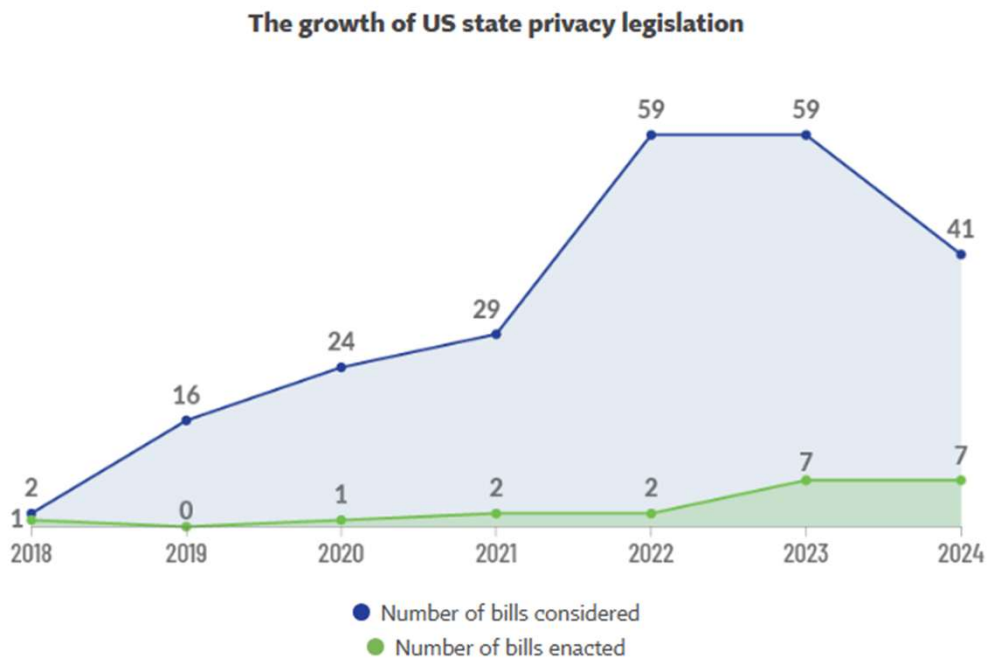
CCPA Expansion *(Enac. Sep 2025, Eff. Jan 2026)*
California's expanded CPRA/CCPA requires regular cybersecurity risk assessments and documentation accessible to regulators as privacy laws grow stricter.

New York's DFS Cyber Rule Updates *(Enac. Nov 2023, Eff. Nov 2025)*
New York's DFS Cyber Rule will require multi-factor authentication, asset inventories, and annual self-certification starting in 2026.

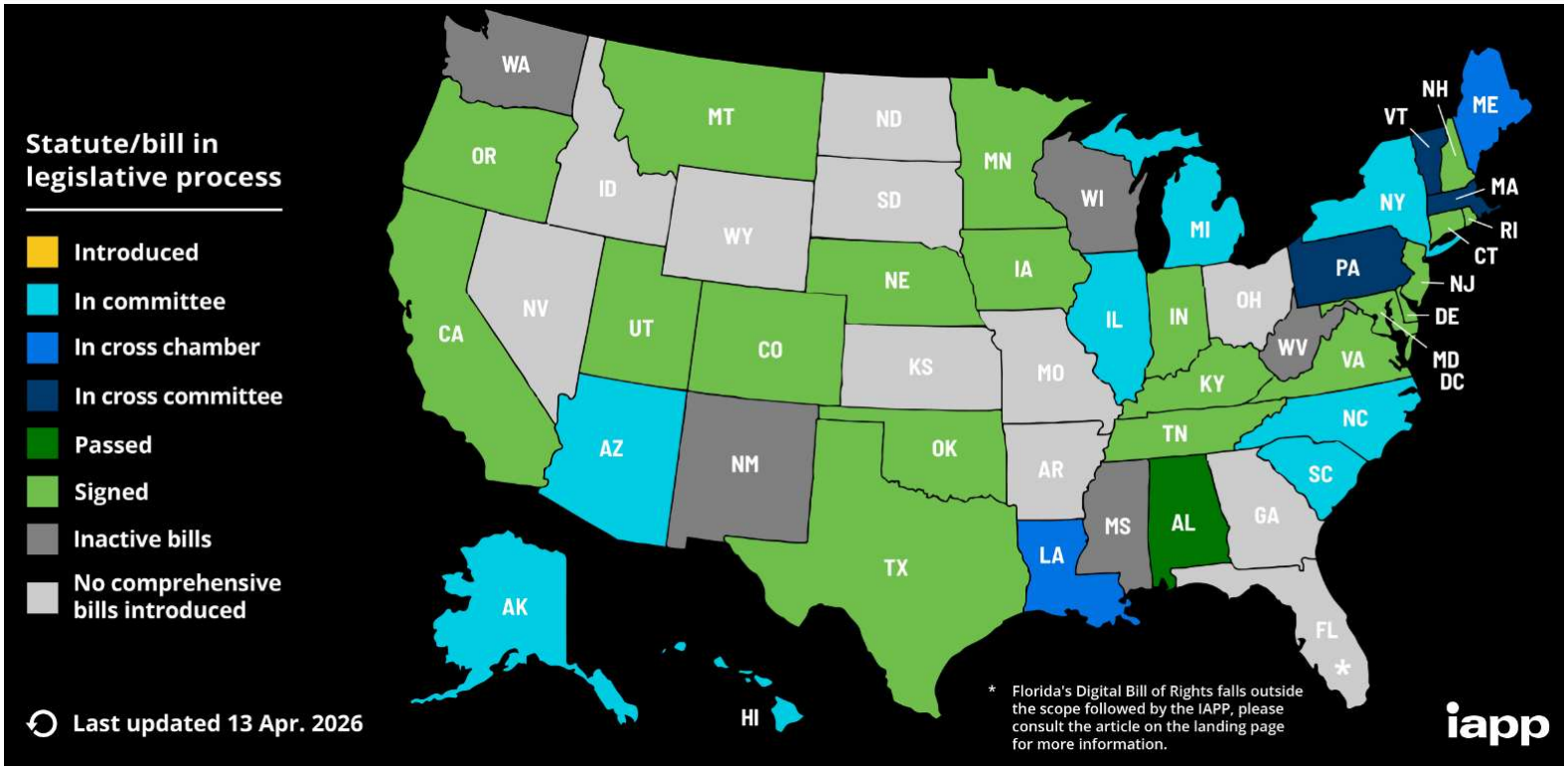
Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) *(Enac. Mar 2022, Eff. 2026)*
Requires certain critical infrastructure organizations to report significant cyber incidents within 72 hours and ransomware payments within 24 hours to federal authorities.

Privacy Trends

Source: IAPP



Privacy Trends



Larson
CERTIFIED PUBLIC ACCOUNTANTS

Common Privacy Legislation Attributes

Consumer Right

- Access
- Correct
- Delete
- Opt-out or in of certain processing and sales
- Portability
- Automated Decision Making
- Civil Legal Action

Business Obligations

- Opt-in default
- Notice/transparent Requirement
- Risk Assessments
- Prohibit Discrimination
- Purpose/processing limitation
  - Retention limits
  - Vendor Management

Larson
CERTIFIED PUBLIC ACCOUNTANTS

Future Threats

Emerging Threats in IT

Quantum Computing Risks

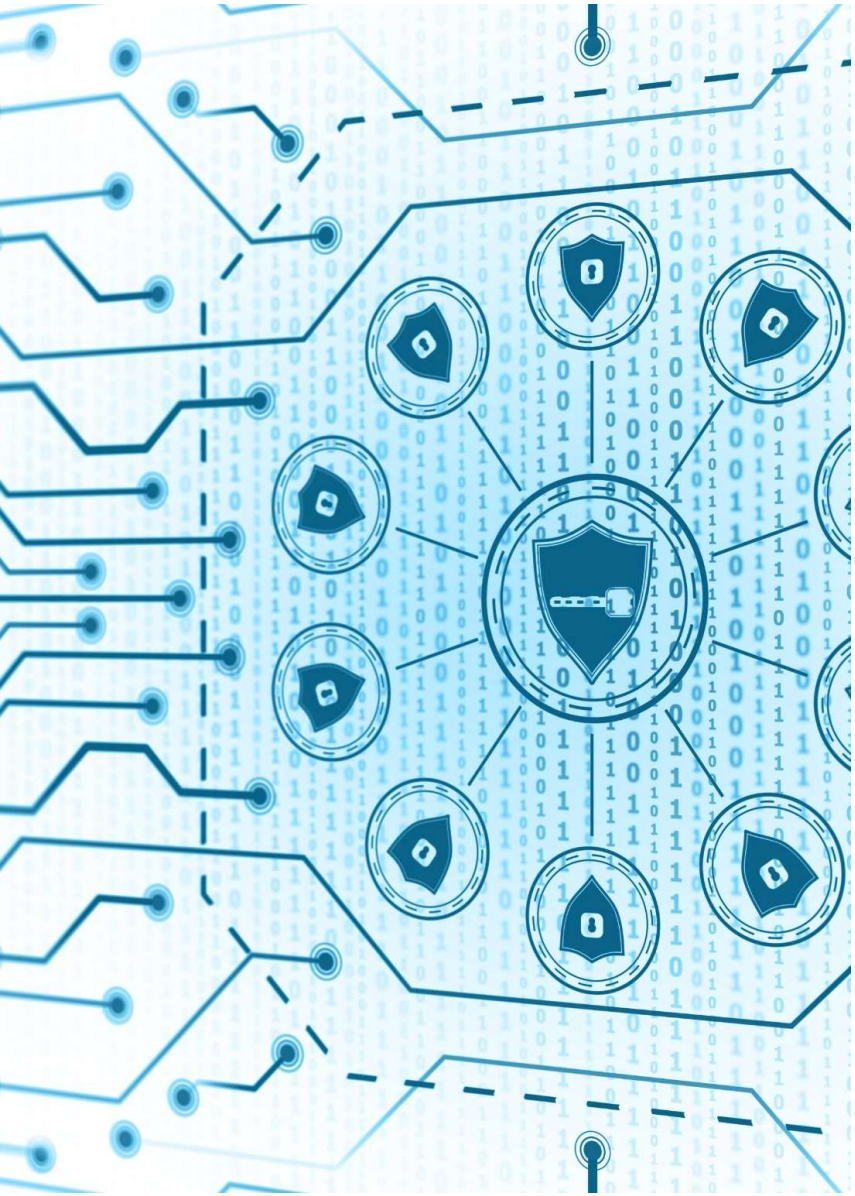
Quantum computers may/will break current encryption standards, increasing the risk of sensitive data being exposed to attackers.

AI-Powered Attacks

Artificial intelligence enables automated, adaptive attacks that can bypass defenses and remain difficult to detect.

IoT/Physical Infrastructure Attacks

Cyber attacks impact physical operations, with the potential to disrupt systems, halt business processes, and create real-world consequences beyond data loss.



Defending Against Emerging Tech Risks

Quantum-Resistant Encryption

Organizations should implement quantum-resistant encryption algorithms to protect sensitive data from quantum computing threats. Start with a cryptographic inventory, then check vendor implementation roadmaps.

Adaptive Security Monitoring

Continuous monitoring and adaptive security systems help defend against AI-powered cyberattacks and quickly respond to threats.

Staff Training and Collaboration

Regular staff training and collaboration with cybersecurity experts strengthen organizational resilience to emerging technological risks.

Operational Resilience Planning

Develop and test business continuity and incident response plans that account for cyber events impacting physical operations, ensuring critical services can continue during disruptions.

Review

- Today's Top Threats
  - Business E-mail Compromise (BEC)
  - Ransomware
  - Social Engineering
  - Generative AI Scams
  - 3rd Party Risk
- Regulation
- Future Threats

Quiz

Larson
CERTIFIED PUBLIC ACCOUNTANTS