Navigating cybersecurity in 2025: trends, controls and mitigating attacks

April 15, 2026

Welcome and introduction

Peter Tsengas, CISA, CISM
Baker Tilly - Risk Advisory Public Sector
IT Director

P: +1 (703) 827 9350
E: peter.tsengas@bakertilly.com

Agenda

- What is happening
- Internal cyber risk factors
- External cyber risk factors
- Cybersecurity trends to consider for 2026
- Benefits of cybersecurity frameworks
- Key takeaways

What is happening

Some of the latest headlines

Why state and local governments are targets for cyberattacks

Experts point to various reasons for the steady increase of cyberattacks against state and local governments. One factor is the number of local governments — 90,075 units — in the U.S., according to the International City/County Management Association (ICMA), an organization for city and county managers and other employees who serve local governments. Out of this total, 38,779 are general purpose governments and are made up of:

- 3,031 county governments
- 19,475 municipal governments
- 16,253 town or township governments

State and local governments are tasked with a combination of major priorities, including overseeing vital services, managing critical infrastructure and responding to their residents' needs. These priorities have also introduced new risks to state and local governments. These governments and their agencies store sensitive information, especially personal information such as names, addresses, driver's license numbers, property tax information, social security numbers and tax and voter records. This also includes the governments' own financial, billing and contractual information.

How communication helps state, local governments prevent and mitigate cyberattacks | Rave Mobile Safety, 05/2022

Some of the latest headlines (cont.)

Most Common Cyber Attacks

Non-payment/non-delivery attacks are the most common US cyber threat since 2020 with 60,113 incidents, which involves fraudsters tricking victims into paying for undelivered goods or services.

	Cyber Attack	Total Attacks (2020-2024)
1	**Non-payment/Non-Delivery**	60,113
2	**Personal Data Breach**	40,523
3	**Phishing/Spoofing**	29,459
4	**No Lead Value**	25,523
5	**Overpayment**	24,945
6	**Extortion**	20,963
7	**BEC**	19,784
8	**Credit Card/Check Fraud**	19,085
9	**IPR/Copyright and Counterfeit**	18,849
10	**Harassment/Stalking**	18,112

+ Show 16 more

The most common cyberattacks and most costly cyberattacks were calculated as the sum total across all states for each attack type.

Table: Ricki Lee, TechInformed • Source: Kiteworks • Created with Datawrapper

Source: Study reveals which U.S. states are most vulnerable to cyber-attacks

Some of the latest headlines (cont.)

Most Costly Cyber Attacks

Business Email Compromise (BEC) is the cyberattack in the United States with the highest financial impact, with losses exceeding $1 billion ($1,747,924,931) since 2020 and an average loss of $88,350 per incident.

	Cyber Attack	Total Losses (2020-2024)	Average Losses Per Attack
1	BEC	$1.75B	88,350
2	Credit Card/Check Fraud	$516.05M	27,039
3	Malware	$237.47M	83,235
4	Personal Data Breach	$217.22M	5,360
5	Lottery/Sweepstakes/Inheritance	$211.42M	13,869
6	Real Estate	$180.69M	12,721
7	Data Breach	$121.16M	12,575
8	Crimes Against Children	$114.28M	56,688
9	Investment	$103.07M	6,423
10	Phishing/Spoofing	$81.56M	2,769

+ Show 18 more

The most common cyberattacks and most costly cyberattacks were calculated as the sum total across all states for each attack type.

Table: Ricki Lee, TechInformed • Source: Kiteworks • Created with Datawrapper

Source: Study reveals which U.S. states are most vulnerable to cyber-attacks

Some of the latest headlines (cont.)

Student, teacher information exposed in PowerSchool software cyberattack

RELATED VIDEO The Better Business Bureau has emphasized the importance of being informed about cybersecurity risks. (Source: WIFR)

By Jordan Gartner
Published: Jan. 8, 2025 at 5:18 PM EST | Updated: Jan. 8, 2025 at 5:34 PM EST

(Gray News) - A popular platform for school districts to keep track of student records and communication with families has been hit by a cyberattack.

PowerSchool, a cloud-based software platform used in K-12 schools for students, parents and educators, announced that it has become aware of a data breach that affected some of its clients last month.

Cyber attack on Harrisburg text alert provider under control

The cybersecurity incident was targeted and was strictly contained. While it didn't impact anything outside of the alert system, it raised concerns.

By Parker Brown
Published: Nov. 26, 2025 at 9:45 PM EST | Updated: Nov. 26, 2025 at 10:16 PM EST

HARRISBURG, S.D. (Dakota News Now) - In Harrisburg, a cyber attack damaged an emergency notification system called CodeRED by Crisis24.

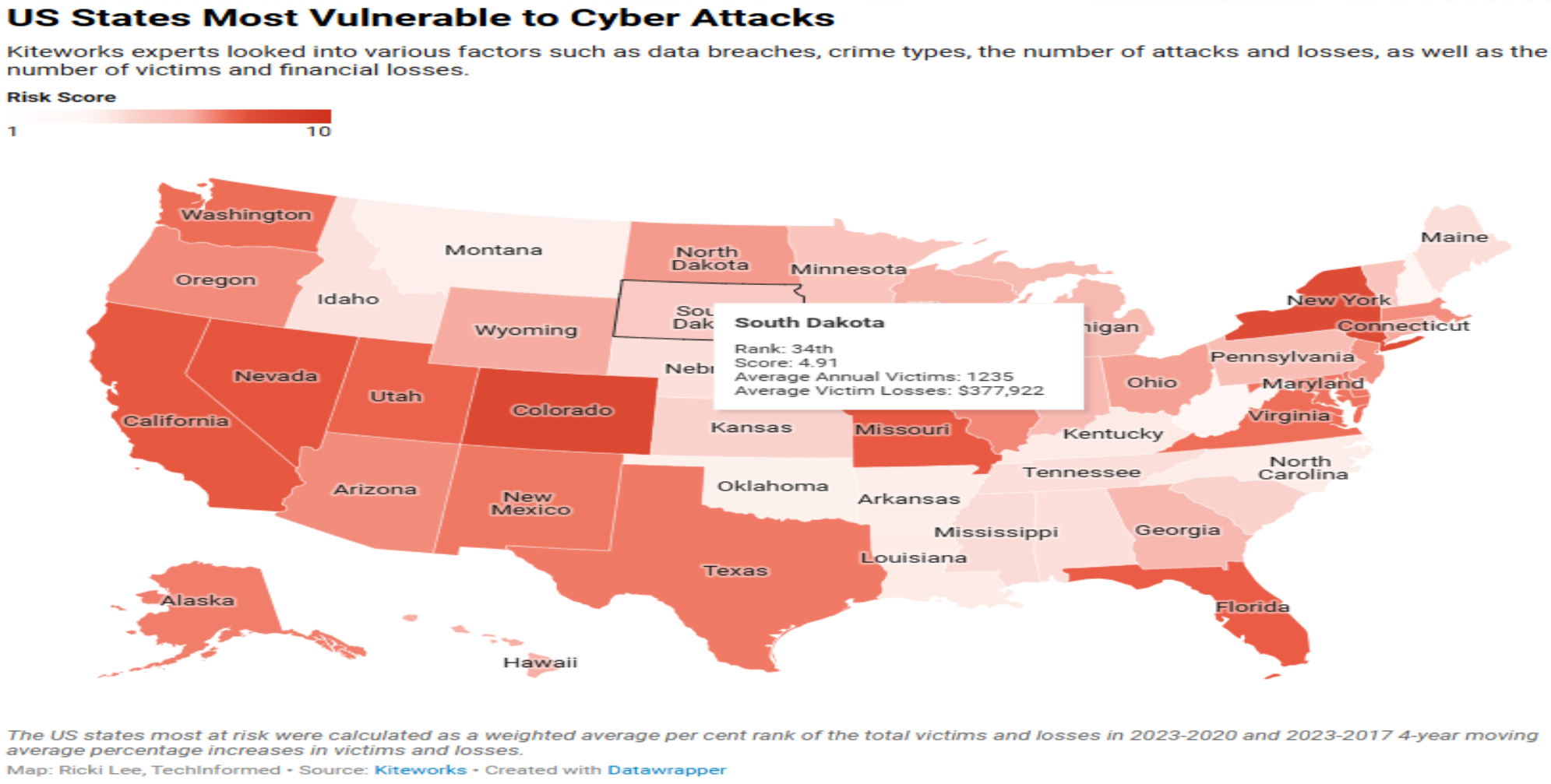
The cybersecurity incident was targeted and was strictly contained within the OnSolve CodeRED environment. While it didn't impact anything outside of the alert system, it does raise some concerns about what information hackers might have access to.

"Unfortunately, I think going forward in the future, this is something that we're just going to have to learn to live with," said Harrisburg Mayor Derick Wenck.

As more services move online, more of your information could be at risk, no matter how secure the provider is. Emergency text notification systems are no different.

Sources:
Student, teacher information exposed in PowerSchool software cyberattack
Cyber attack on Harrisburg text alert provider under control

Some of the latest headlines (cont.)



Source: Study reveals which U.S. states are most vulnerable to cyber-attacks

TOP 5

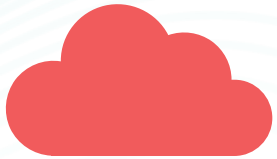
Biggest cyber risks

Ransomware

Remember Colonial Pipeline in 2021?

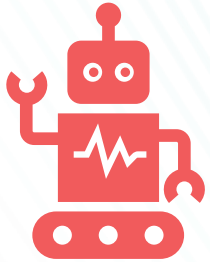
Outdated software

Many governments still have old “crusty” software



Supply chain

Vendor access to key systems



Internet of things (IoT) & industrial control systems (ICS)

New systems introduce new problems and risk

Phishing & social engineering

People are the weakest link

Internal and external cyber risks

HOW IS YOUR IT TEAM MANAGING YOUR INTERNAL CYBER RISKS?

Internal cyber risks

Malicious insiders	Software development	Network security
Vulnerability management	User authentication	Data protection
Technical debt	Privileged accounts	End-user training

HOW IS YOUR IT TEAM MANAGING YOUR EXTERNAL CYBER RISKS?

External cyber risks

Nation states	Advanced persistent threats	Social engineering
Supply chain risk	Ransomware	System integrations
Cloud services	Malware	Identity and access management

Cybersecurity trends to consider for 2026

Cybersecurity trends to consider for 2026 (cont.)

As organizations refine their AI strategies to align with governance, risk, and performance goals, Info-Tech's AL Trends 2026 report highlighted five key developments that will influence how enterprises deploy and manage AI in 2026:

1. Foundational AI Principles Will Rewrite Organizational DNA
   - AI Strategies will be informed by an emerging set of principles.
   - Nearly 60% of leaders surveyed by Info-Tech say they will introduce or update AI principles in 2026, and 44% have already embedded Responsible AI guidelines into their policy and training frameworks.

2. From copilots to the vibe coding: AI will continue to reinvent IT
   - The ecosystem of AI solutions for IT will grow with the introduction of new categories.
   - Over half of the enterprises (54%) surveyed by Info-Tech report integrating generative AI into software development workflows, while one in three plan to introduce AI-based "vibe coding" or autonomous code generation pilots in 2026.

3. Agnetic AI will come of age and power the exponential enterprise
   - Agentic AI will increase in adoption and enable outcomes across the organization, powering, exponential growth and change.
   - Sixty-four (64%) of organizations surveyed by Info-Tech are experimenting with agnetic AI for analytics and automation, yet fewer than 25% have implemented formal agent monitoring or escalation procedures.

Sources:
AI Trends 2026 Report: Risk, Agents, and Sovereignty Will Shape the Next Wave of Adoption, Says Info-Tech Research Group

Cybersecurity trends to consider for 2026 (cont.)

As organizations refine their AI strategies to align with governance, risk, and performance goals, Info-Tech's AL Trends 2026 report highlighted five key developments that will influence how enterprises deploy and manage AI in 2026:

4. Risk management will be the price of admission for AI
   - Adoption of AI risk management programs will be driven by the potential new risks that AI applications can introduce.
   - 68% of leaders surveyed by Info-Tech now identify AI risk governance as their top operational priority, up from 39% last year.

5. AI will hang in the balance between freedom and control
   - AI sovereignty is becoming a geopolitical priority as nations pursue local models and data independence.
   - 72% of leaders surveyed by Info-Techy list data sovereignty and regulatory compliance as their top AI-related challenged for 2026, up from 49% last year.

Sources:
AI Trends 2026 Report: Risk, Agents, and Sovereignty Will Shape the Next Wave of Adoption, Says Info-Tech Research Group

Key AI Risks and Threats to Consider

- Data Poisoning
- Model Inversion
- Privacy Leakage
- Backdoor Attack
- Evasion Attacks
- AI-Enhanced Social Engineering
- API Attacks
- Model Poisoning
- Hardware Vulnerabilities

Cybersecurity trends to consider for 2026 (cont.)

Below are five key strategies to consider for minimizing AI threats:

1. Data Validation
2. Enhance Model Security
3. Strong Access Controls
4. Regular Security Audits
5. Ethical AI Practices

Sources:
Top 14 AI Security Risks in 2025

Benefits of cybersecurity frameworks

Benefits of cybersecurity frameworks

Implementing cybersecurity frameworks and standards offer organizations numerous benefits:

1. Improved security posture	5. Improved communication
2. Reduced risk	6. Cost-effective security
3. Enhanced compliance	7. Operational efficiency
4. Increased customer trust	8. Continuous improvement

Cybersecurity frameworks provide a structured approach to managing cyber risks, making it easier for organizations to identify vulnerabilities, establish strong security measures and develop response plans.

Cybersecurity frameworks and standards to know

Payment Card Industry Data Security Standard (PCI DSS)

System and Organization Controls (SOC) 2®

National Institute of Standards and Technology (NIST): AI Risk Management Framework (AI 600-1)

National Institute of Standards and Technology (NIST): 800-53, 800-171 and the Cybersecurity Framework (CSF) 2.0

Key takeaways

Key takeaways

Importance of proactive cybersecurity measures

Employee training and awareness

Incident response planning

Securing operations technology

Collaboration and information sharing

Q&A

Peter Tsengas, CISA, CISM

Baker Tilly - Risk Advisory Public Sector
IT Director

P: +1 (703) 827 9350
E: peter.tsengas@bakertilly.com

Scan here to contact