State of Illinois
State Internal Audit Advisory Board

bakertilly

Navigating cybersecurity in 2025: trends, controls and mitigating attacks

October 21, 2025

Welcome and introduction

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

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

Agenda

- What is happening
- Internal and external cyber risks
- 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.)

CYBERSECURITY

Illinois Human Services Breach Compromises Data of 1M

The data breach last year by an outside entity resulted in the accessing of files that included Social Security numbers. Separately, hackers obtained the public assistance account information of more than 1 million people.

January 02, 2025 • Commercial-News

Shutterstock

(TNS) — On April 25, the Illinois Department of Human Services (IDHS) experienced a privacy breach. An outside entity, through a phishing campaign, gained access to multiple employee accounts, and files associated with the accounts. The files included the Social Security numbers (SSNs) of 4,701 customers and three employees.

Separately, public assistance account information (name, public assistance account number, and some combination of address, date of birth, Illinois State Board of Education Student Information System ID number, Recipient Identification Number, and cell phone number) was accessed for 1,118,993 customers. That information did not include SSNs.

On May 3, IDHS, in partnership with the Illinois Department of Innovation and Technology (DoIT), determined the incident was a reportable breach of security under PIPA.

February phishing campaign compromised Illinois health data, department says

A February 11 cyberattack compromised the health data of nearly 1,000 people, announced the Illinois Department of Healthcare and Family Services.

BY SOPHIA FOX-SOWELL • JUNE 6, 2025

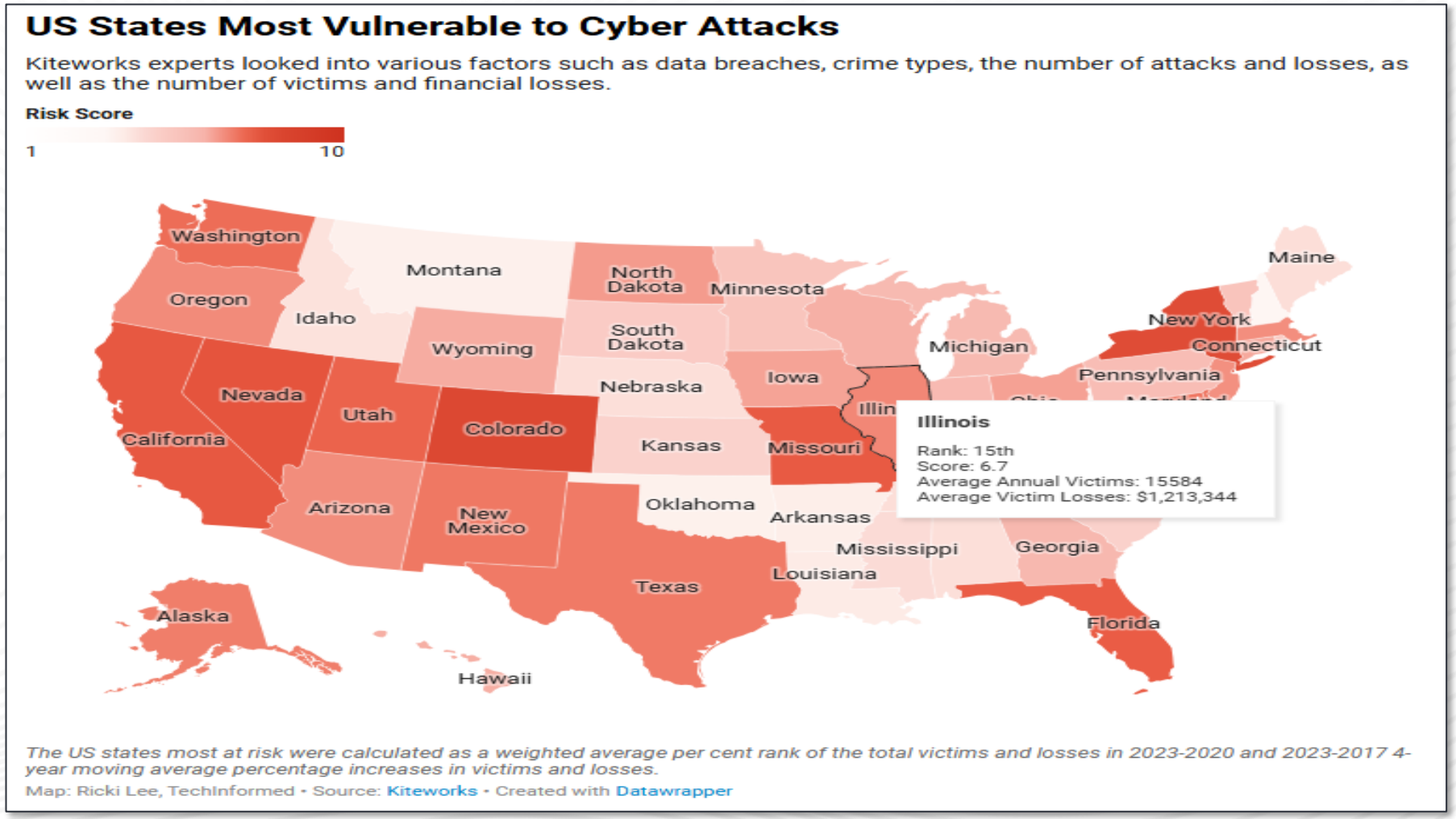
Listen to this article 2:23 Learn more.

(Getty Images)

The Illinois Department of Healthcare and Family Services on Friday announced a data breach resulting from a phishing attack earlier this year that compromised the personal information of 933 people, including 564 Illinois residents.

Sources:
Illinois Human Services Breach Compromises Data of 1M
February phishing campaign compromised Illinois health data, department says | StateScoop

Some of the latest headlines (cont.)



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

TOP 5

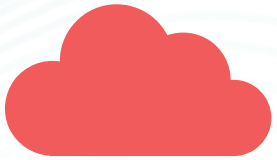
Biggest cyber risks

Ransomware

Remember Colonial Pipeline in 2021?

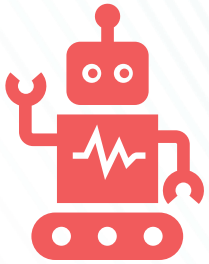
Outdated software

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

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 to know

Payment Card Industry Data Security Standard (PCI DSS)

System and Organization Controls (SOC) 2®

Cybersecurity Maturity Model Certification (CMMC)

National Institute of Standards and Technology (NIST), including 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 - Public Sector IT Risk Advisory Director

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

Scan here to contact