TEXAS RE

Data Breach Response

Rebecca Jones
Mullen Coughlin

August 26, 2025

Antitrust Admonition

Texas Reliability Entity, Inc. (Texas RE) strictly prohibits persons participating in Texas RE activities from using their participation as a forum for engaging in practices or communications that violate antitrust laws. Texas RE has approved antitrust guidelines available on its website. If you believe that antitrust laws have been violated at a Texas RE meeting, or if you have any questions about the antitrust guidelines, please contact the Texas RE General Counsel.

Notice of this meeting was posted on the Texas RE website and this meeting is being held in public. Participants should keep in mind that the listening audience may include members of the press, representatives from various governmental authorities, and industry stakeholders.

Upcoming Texas RE Events

September 9, 2025

Internal Controls

October 20, 2025

PUCT Cybersecurity Program

October 21, 2025

IBR Registration and Applicable Standards

Upcoming Texas RE Events

September 17, 2025

Q3 MRC and Board Meetings

October 1, 2025

Winter Weatherization Workshop

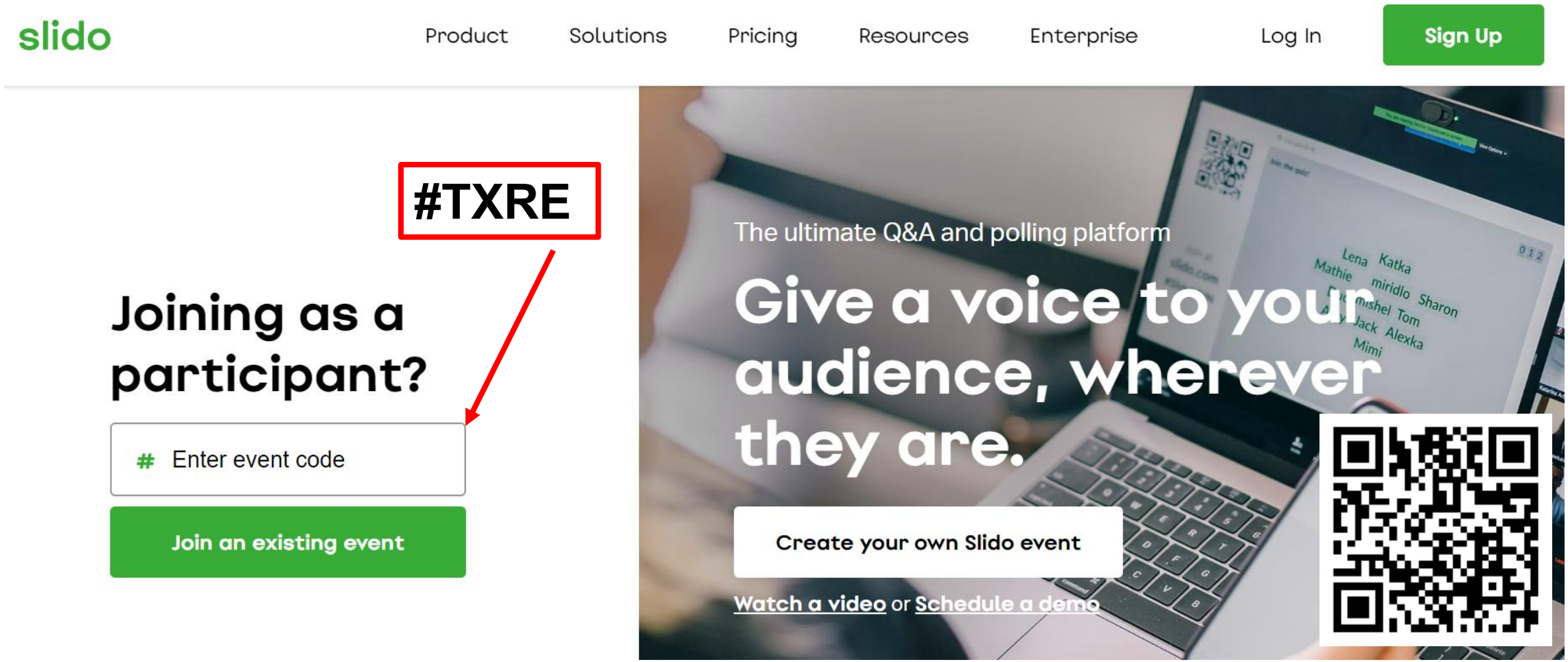
November 5, 2025

Fall Standards, Security, & Reliability Workshop

Upcoming ERO Enterprise Events

Date	Event
September 3	Reliability in the West: Large Load System Performance (WECC)
September 3	Misoperations: Submitting Quality Information to MIDAS (MRO)
September 8	Fall Reliability & Security Summit (RF)
September 9	System Operator Conference #3 (SERC)
October 14, 2025	Reliability and Security Workshop (WECC)

Slido.com


slido
Product
Solutions
Pricing
Resources
Enterprise
Log In
Sign Up
#TXRE
Joining as a participant?
Enter event code
Join an existing event
The ultimate Q&A and polling platform
Give a voice to your audience, wherever they are.
Create your own Slido event
Watch a video or Schedule a demo

MULLEN COUGHLIN

Cybersecurity Risks & The Incident Response Process

Presented by: Rebecca Jones, Mullen Coughlin

August 26, 2025

Agenda

- Incident Risks & Trends
- Incident Response Roadmap
- Best Practices
- Considerations

Cyber Event Trends & Statistics

Cyber Threat Overview

- Malicious attacks
  - Ransomware; extortion
- Employees
  - Phishing campaigns; social engineering (including deep fakes using AI); wire fraud
  - Negligent failure to follow or learn policies and procedures
- Business Partners / Supply Chain attacks
  - Attacks result in compromise to networks and/or data shared with the business partner

Current Case Trends

- Ransomware
  - Double Extortion
  - Harassment
  - Increased public exposure
- Business Email Compromise
  - Wire Fraud/Personal Information Harvesting
  - Most frequent type of incident MC handles
- Software Exploits or Vulnerabilities
  - Appliance & Application Zero-Days – *e.g.*, Cisco, SolarWinds, Fortinet, SharePoint
  - CISA Known Exploited Vulnerability Catalog
- Third-Party Vendor Events
  - MOVEit, Change Healthcare, Ascension Healthcare, Snowflake

Incident Type

2022

Incident Type	Count
Business Email Compromise (BEC) – Total	1,075 (36%)
BEC – Other	731
BEC – Wire Fraud	344
Ransomware	735 (25%)
Network Intrusion	382 (13%)
Vendor Breach	315 (11%)
Other	245 (8%)
Inadvertent Disclosure	207 (7%)
Total	**2,959 (100%)**

2023

Incident Type	Count
Business Email Compromise (BEC) – Total	1,343 (34%)
BEC – Other	996
BEC – Wire Fraud	347
Ransomware	883 (23%)
Vendor Breach	749 (19%)
Other	403 (10%)
Network Intrusion	323 (8%)
Inadvertent Disclosure	218 (6%)
Total	**3,919 (100%)**

2024

Incident Type	Count
Business Email Compromise (BEC) – Total	1,601 (38%)
BEC – Other	1,224
BEC – Wire Fraud	377
Ransomware	1,011 (24%)
Vendor Breach	747 (18%)
Other	346 (8%)
Network Intrusion	322 (7%)
Inadvertent Disclosure	228 (5%)
Total	**4,255 (100%)**

2025 (through June)

Incident Type	Count
Business Email Compromise (BEC) – Total	803 (38%)
BEC – Other	617
BEC – Wire Fraud	186
Ransomware	556 (26%)
Vendor Breach	357 (17%)
Network Intrusion	174 (8%)
Other	161 (7%)
Inadvertent Disclosure	80 (4%)
Total	**2,131 (100%)**

Ransomware Incidents

2022	
Number of RW Incidents	735 (25%)
Number of RW Incidents Paid	114 (16%)
Average Ransom Demand	$2,241,753
Average Ransom Payment	$438,901
Median Ransom Payment	$208,774
Ransom Payment Reason	Delete Only – 26 (23%) Key and Delete – 48 (42%) Key Only – 40 (35%)

2023	
Number of RW Incidents	883 (23%)
Number of RW Incidents Paid	156 (18%)
Average Ransom Demand	$2,180,723
Average Ransom Payment	$823,357
Median Ransom Payment	$200,000
Ransom Payment Reason	Delete Only – 50 (32%) Key and Delete – 66 (42%) Key Only – 40 (26%)

2024	
Number of RW Incidents	1,011 (24%)
Number of RW Incidents Paid	161 (16%)
Average Ransom Demand	$1,755,468
Average Ransom Payment	$452,530
Median Ransom Payment	$220,000
Ransom Payment Reason	Delete Only – 66 (41%) Key and Delete – 61 (38%) Key Only – 34 (21%)

2025 (through June)	
Number of RW Incidents	556 (26%)
Number of RW Incidents Paid	27 (5%)
Average Ransom Demand	$1,059,132
Average Ransom Payment	$327,915
Median Ransom Payment	$175,000
Ransom Payment Reason	Delete Only – 9 (33%) Key and Delete – 9 (33%) Key Only – 9 (33%)

Business Email Compromise Incidents

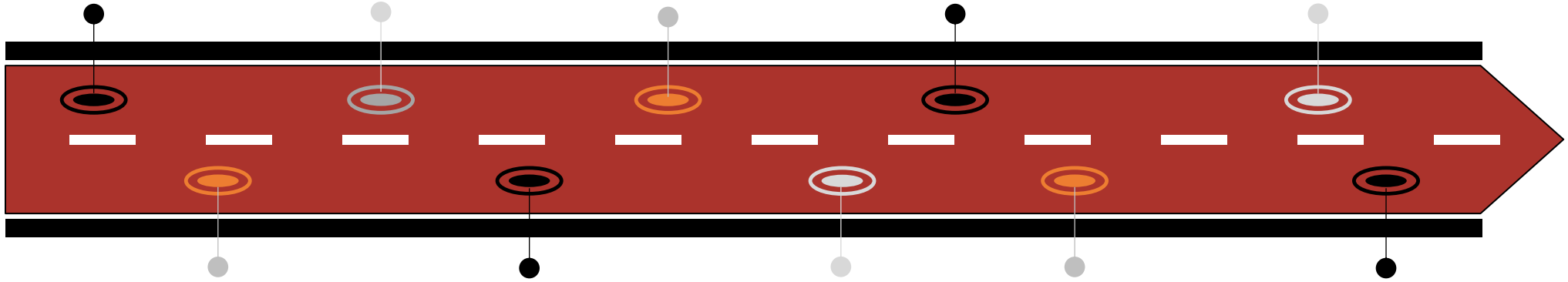
2022	
Number of BEC Incidents	1,075 (36%)
Number of BEC-WF Incidents	344 (32%)
Average Amount Fraudulently Wired	$374,434
Median Amount Fraudulently Wired	$144,000

2023	
Number of BEC Incidents	1,343 (34%)
Number of BEC-WF Incidents	347 (26%)
Average Amount Fraudulently Wired	$824,704
Median Amount Fraudulently Wired	$148,867

2024	
Number of BEC Incidents	1,601 (38%)
Number of BEC-WF Incidents	377 (24%)
Average Amount Fraudulently Wired	$442,961
Median Amount Fraudulently Wired	$154,622

2025 (through June)	
Number of BEC Incidents	803 (38%)
Number of BEC-WF Incidents	186 (23%)
Average Amount Fraudulently Wired	$506,373
Median Amount Fraudulently Wired	$120,000

The (Potential) Roadmap



Incident Response Process

- Typical Incident Response process:
  - Contact carrier and/or broker to discuss filing a claim
  - Mullen Coughlin retained to direct incident response and investigation
  - Mullen Coughlin to engage forensics on your behalf, getting approval from carrier on vendor selection if needed
  - Forensics will start investigation once engaged; typically start with containment efforts and evidence collection
    - May include a separate TA negotiator if ransomware
    - Investigation takes approximately 1-4 weeks; recovery can take longer
  - Some incidents will require reporting to certain regulators early on
    - Consider law enforcement reporting
  - Decision points flow from findings and recommendations of forensic investigation and other intel, such as TA negotiations
  - Mullen Coughlin to identify legal notice requirements and coordinate notice process
  - Recovery process is ongoing throughout the above steps until completion

Considerations- Incident Impacts

- Not all incidents result in legal notice obligations; depends upon findings of forensic investigation, other available information, and applicable legal framework
  - This will be determined by legal counsel
- Many incidents do result in notice to the individuals whose information was impacted, and to applicable federal, state, and industry regulators
  - Impacted information could pertain to employees, customers, business partners, other entities, etc.
- Reputational impact
  - Loss of business, negative social media attention
- Litigation is now common and expected as result of notice

Best Practices- Incident Response

Best Practices: Pre-Incident

- Ensure experience on Security Incident Response Team (SIRT)
  - Test regularly to ensure all team members understand the IRP and process to set up for an efficient response
  - Understand who is responsible for certain decision points
- Talk to your IT security staff and address concerns early
  - Gain an appreciation of the many challenges and risk landscape
- Identify items/processes needed to facilitate business continuity and ensure availability
- Organize contractual notice obligations/contracts to avoid missing deadlines
- Prepare and update your Incident Response Plan (IRP) annually or if material change in business practices
- Document the training and enforcement measures being taken

Best Practices: Incident Response

- Engage third-party forensics and use counsel to establish attorney-client privilege early in process
  - Counsel engages and directs third-party forensics and other vendors so that, in the event of litigation or regulatory investigation, all documents and communications are not discoverable
    - Third-party forensics will perform analysis and provide opinions and guidance
  - Protect attorney-client privilege – do not share forensic reports, legal analysis and drafts with clients or third parties if not absolutely necessary
  - Limit internal documentation to facts and only as needed
    - Use verbal communications instead of written where appropriate
- Do not use term "Breach" lightly — this is a statutorily defined legal term and the use and admission of which has consequences

Best Practices: Incident Response

- Do not rush to make public statements
  - An inability to answer questions that will inevitably follow can hinder the investigation and create additional risks
  - If your notice goes out four (4) hours after discovery, there will be people who accuse you of delay, so "delay" is unavoidable
  - Ensure understanding of facts before making statements about impact, or avoid public statements altogether
- Prepare for litigation and regulatory investigation — Preserve all relevant documents
- Implement data security improvements *prior* to being asked by a regulator

Litigation Trends

Data Privacy and Security Investigations

Typically Based on New, Existing and Updated Regulations

- Inquiries (expanding in volume, scope and intensity)
- Requests and responses
- Document productions, interviews, formal proceedings
- Negotiations (consent orders including fines)

Political Considerations

- Unsympathetic Defendant / Repeat Offender
- Size and type of population affected
- Elections / Press Releases

Law Enforcement

- U.S. Department of Justice (DOJ)
- Federal Bureau of Investigation (FBI)
- U.S. Secret Service (USSS)
- State Attorneys General (AGs)

Federal Regulators

- Consumer Financial Protection Bureau (CFPB)
- U.S. Department of Defense (DoD) and DoD Cyber Crime Center (DC3)
- U.S. Department of Homeland Security (DHS)
- U.S. Securities and Exchange Commission (SEC)
- Federal Deposit Insurance Corporation (FDIC)
- Federal Trade Commission (FTC)
- Federal Reserve

State Regulators

- New York Department of Financial Services (NYDFS)
- California Privacy Protection Agency (CPPA), etc.

Initiation of Data Breach Litigation

- Required Notification to Individuals and Regulators
  - Definition of "Security Breach"
  - Notification Triggering Language
    - Access + Acquisition
    - Potential Harm
- Publication of Incidents and Scope by Regulators
  - SEC filings; media attention
  - Numerous State AGs post incident reports online
- Plaintiff Recruitment
- Volume of Litigation
  - Class Size
  - Type of Incident (If Known)
    - Publication of Class Member Data?
  - Data Elements
  - Type of Defendant

Litigation Trends

- Minimum class size decreasing
- Causes of action expanding
  - Website tracking technologies & data breaches
- Cases are settling, not going to trial