

A YEAR OF PRIVACY AND CYBERSECURITY:

A Look Back, A Look Around, and A Look Ahead



As the digital landscape continues to evolve and technology advances, privacy and cybersecurity remain central concerns for individuals, businesses, and regulators. There have been significant developments in privacy regulations and government enforcement actions, major data security incidents, and cybersecurity innovations. From the rise of sophisticated ransomware attacks to the implementation of new state privacy laws, the landscape has been marked by both challenges and progress. Here, we discuss our experience in the past year in privacy and cybersecurity, explore some landmarks in the current environment, and make a few predictions on possible future developments.

A Look Back at 2024

In April, BakerHostetler will publish its eleventh annual Data Security Incident Response Report (“DSIR Report”), distilling insights and metrics from more than 1,250 data incidents our firm helped clients manage in 2024. The DSIR Report is designed, in part, to help develop cybersecurity measures, incident response plans, and information governance practices. Some highlights from our current analysis of the DSIR Report data are below.

Ransomware preparedness and response may be improving.

Ransomware has long been a scourge, and the effects of an attack can be devastating. Unprepared organizations hit with ran-

somware encryption may need weeks to recover full functionality. During this time, the attack may be highly visible, and the encryption can make it difficult or impossible to deliver for clients, customers, and other stakeholders. Compounding these challenges, threat actors often engage in a double-extortion model: data is exfiltrated prior to encryption and payment demanded not only for a tool to decrypt, but also to prevent publication of the stolen information. Victim organizations also must inform affected individuals and regulators according to applicable data breach notification laws.

In 2024, though, the effects of ransomware attacks were somewhat suppressed. Most of the network intrusions our firm handled in 2024 involved both data theft and ransomware encryption. Even so, the proportion of victims that paid a ransom to purchase a decryption tool did not increase significantly when compared to 2023, and in 2024, the time to recover from a ransomware attack once again saw a year-over-year decrease. This suggests organizations are continuing to improve backup management and recovery processes, as the availability of and time to recover from viable backups can be key drivers for an organization evaluating whether to pay a ransom. Additionally, compared to 2023, the cost and time to complete a forensic investigation both decreased in 2024, and fewer ransomware events involving data theft resulted in notice to individuals. This may show not only that forensic investigators are increasingly efficient, but also that organizations continue to implement information management strategies that help control unauthorized access to sensitive data.

Ransomware continues to be a risk, but organizations appear to be implementing measures that can reduce the impact of an attack. Multifactor authentication (“MFA”) and a properly configured endpoint detection and response tool (“EDR”) can help prevent access or detect potentially malicious activity. Managing access permissions to the minimum necessary for a user’s role and auditing accounts to remove privileges not needed can help to contain threats in the event of a network intrusion. Appropriate data retention poli-

cies and procedures can help to prevent the exposure or exfiltration of sensitive data. Consistently following best practices for backup procedures and testing, such as the “3-2-1 backup rule” (three copies: one live/in production; two others on different devices/media; one of those at an offsite location), can help to eliminate the need for a decryption tool and reduce recovery time in the event of ransomware encryption.

A renaissance for large fraudulent fund transfers?

Unauthorized actors use a variety of techniques to gain access to systems and networks, but social engineering continues to be a leading cause of financial loss for organizations. As an example of one common method, an attacker may send a phishing email purporting to be from a known or legitimate source with a link to access a document or view a secure message. The link takes the recipient to a webpage that appears legitimate, such as a spoofed Microsoft login page, and asks them to sign in to review the content. Upon entering their credentials, the recipient sees a login error but has granted an unauthorized actor access to their email account.

Phishing attacks such as this were a significant vector for unauthorized actors to gain access to email accounts in 2024. As a potential corollary, 2024 also saw an increase in the total amount of funds diverted by criminals when compared to 2023, as well as the average amount that was the subject of a misdirected transfer. After gaining access to an email account, unauthorized actors were seen to impersonate counterparties to change payment instructions and divert funds. They concealed their activity from users by creating rules to hide legitimate messages from the real counterparty.

Organizations can help to protect against these kinds of attacks by employing technical solutions, adding additional controls, and raising awareness. Multi-factor authentication, voice-verification for changes to payment instruction and post-transfer verbal confirmation, and additional employee training and testing of protocols are all measures that can help to reduce the risk of financial loss at the hands of an email phisher.

Vendor incidents are still a risk that must be managed.

Once again in 2024, approximately 25% of the incidents we saw involved assisting clients with managing the impacts of outside vendors and service providers. This trend shows no sign of slowing. We continue to assist clients whose service providers had high-profile incidents, such as Change Healthcare and Snowflake; attacks on software and systems, such as secure file transfer protocol applications (“SFTPs”), including Accellion, MOVEit, and Cleo (among others); and other third parties, such as managed service providers. The continuing prevalence of third-party data incidents highlights the importance of incorporating a robust vendor management program into information management and cybersecurity strategies.

To manage risks posed by third-party service providers, organizations should consider three key elements for their vendor management program: pre-selection diligence, contractual standards, and performance oversight. Assessing and classifying

the risk level of each vendor through questionnaires, onsite reviews, audits, or third-party risk scoring should be a regular part of pre-engagement diligence. After a vendor is selected for engagement, the contract terms should address the organization’s privacy and security needs, which may include provisions concerning the data elements involved, the availability of the data to the organization, the vendor’s business continuity plan, and the rights and obligations of each party in the event of a data incident at the vendor. During the engagement, the organization should undertake to monitor and review the vendor’s performance to ensure that the agreed-upon measures and practices are in place and, when the engagement ends, take the appropriate steps to ensure its data is secure to mitigate or eliminate the impacts in the event the vendor has a post-engagement incident.

Current Trends in Privacy and Cybersecurity *Comprehensive Privacy Legislation: The New Black-Letter Law Sweeping the Nation*

While certain federal laws govern privacy



HAWASH
HOUSTON
— M E D I A T I O N —

MEDIATION | ARBITRATION | EARLY DISPUTE RESOLUTION

To schedule, contact:
Teresa Martinez, Case Manager at
Teresa@HoustonMediation.com
713.658.9015

THE NATIONAL ACADEMY OF
DISTINGUISHED NEUTRALS

CDM
CONFIDENTIAL
DISTINGUISHED
NEUTRAL
2025
ELAA'S MEDIATION
CONFIDENTIALITY ASSOCIATION

AMERICAN ARBITRATION ASSOCIATION
PANEL MEMBER 2024

711 W. Alabama St., Houston, Texas 77006
www.HoustonMediation.com

in particular industries or in connection with some types of transactions, the United States Congress has yet to pass generally applicable federal privacy legislation. State legislatures are filling the gap with their own comprehensive privacy laws that address consumer privacy rights and business obligations.

California passed the first such law in 2018, the California Consumer Privacy Act (“CCPA”), and 19 states now have a comprehensive consumer privacy law on the books. Seven of these were signed into law in 2024. The Texas Data Privacy and Security Act (“Texas DPSA”), which is the Texas comprehensive consumer privacy law, was passed in 2023 and became effective in July 2024. Comprehensive privacy laws become effective in seven more states in 2025. There are also 14 states with comprehensive privacy laws at some stage of the legislative process.

While the scope of comprehensive privacy laws varies by state, laws typically recognize that consumers have the right to access, correct, or delete personal information maintained by a business (or “data controller”), to opt out of having their personal information processed, and to request their personal information be disclosed to them in a common file format for portability. Many also require the data controller to provide notice to consumers about how their data will be used, make opt-in (rather than opt-out) the default position for sale of personal information of consumers under a certain age, conduct formal risk assessments of their privacy and security measures, and prohibit discrimination against consumers exercising their rights under these laws.

Some states have comprehensive privacy laws featuring unique provisions. For example, Oregon’s comprehensive privacy law allows an individual to request a list of third parties to which the data controller discloses their personal data. The Texas DPSA states that it applies to any business which produces goods or provides services to a resident of Texas that is not a “small business” under the U.S. Small Business Administration standards, rather than establish applicability based on a certain threshold of data processed.

In short, a federal comprehensive privacy law may lay beyond the horizon. For now,

state legislatures are taking up the mantle to put forward and pass legislation for their own constituencies. The result has been a patchwork of regulations, some of which include novel approaches, which can present compliance challenges.

New Frontiers in State Investigation and Enforcement

As comprehensive privacy laws become more widespread across the nation, state attorneys general are ramping up their enforcement efforts. Texas has been notably active in investigations related to location and biometric data, utilizing Texas consumer protection laws, and the Texas DPSA may provide another tool for investigation and enforcement.

State attorneys general are also beginning to explore whether businesses are using artificial intelligence (“AI”) systems in ways that violate privacy protections or fail to provide adequate transparency and consent mechanisms. In September 2024, an AI company in the health care industry entered into an Assurance of Voluntary Compliance (“AVC”) with the Texas Attorney General in connection with alleged violations of the Texas Deceptive Trade Practices Act (“Texas DTPA”). Additionally, in February 2025, the Texas Attorney General’s office opened an investigation of DeepSeek, a China-based AI company, for purported violations of Texas law.

With the confluence of state data privacy laws and the increasing use of AI in data processing and decision-making, companies that develop and use AI will likely need to address a range of privacy issues to meet their compliance goals. These may include how AI interacts with personal data and whether consumers are being properly informed about how their data is being used in AI systems. As AI continues to be a significant tool for businesses, privacy laws are likely to be significant tools state regulators use to examine the role of AI in data processing.

Wire Fraud and Business Email Compromise: An Evolving Role for Federal Law Enforcement

A business email compromise, or “BEC,”

involves the manipulation or hijacking of corporate email systems to deceive employees into transferring funds to criminals. These incidents can involve impersonation of a vendor or known party, as discussed above, or even impersonation of an executive instructing a subordinate to wire money, often under the guise of urgency or confidentiality. The sophistication of these incidents has increased over time, with cybercriminals using social engineering tactics and technical methods to gain access to email accounts and conduct fraudulent wire transfers.

As noted above, in our experience, wire fraud related to BECs remains a major concern. Law enforcement agencies have had to evolve their strategies to address the growing threat posed by these crimes. Traditionally, the U.S. Secret Service has been tasked not only with protecting national leaders but also safeguarding the integrity of U.S. currency. However, as cybercrime has grown, so too has the Secret Service’s role in protecting the nation’s financial infrastructure. The agency has increasingly taken on the responsibility of investigating financial fraud cases, including wire fraud tied to BECs, and is focusing efforts on a proactive approach to email-based scams and wire fraud.

A key element in the Secret Service’s evolving strategies to respond to cybercrime is its Global Investigative Operations Center (“GIOC”), which plays a pivotal role in helping to recover funds for victims of fraud, including BEC-related losses. The GIOC recently announced that it will focus efforts on cases involving more than \$10,000 which are less than 30 days old. While it is still important to report all fraudulent transfers, this prioritization is a direct response to the growing sophistication and frequency of these crimes aimed at helping to ensure that law enforcement resources are well-positioned to intervene swiftly in high-value cases and increase the chances of recovering stolen funds.

Another aspect of the Secret Service’s strategy has been an emphasis on collaboration. The Secret Service has partnered with local, state, and international agencies to share intelligence and resources. Working with the FBI, the Department of

Homeland Security, and other government agencies, as well as private sector firms, the Secret Service continues to build a collaborative network to be better equipped to tackle the complex nature of wire fraud and email compromise.

Additionally, the Secret Service has implemented public awareness campaigns aimed at educating businesses and individuals on the risks of BECs and wire fraud. These initiatives encourage better cybersecurity practices, which can reduce the likelihood of become a victim.

Predictions for the Coming Year

State Enforcement Activity Will Increase

State governments continue to be a driving force in privacy and compliance. The enactment of comprehensive state privacy laws provides another tool for investigations and enforcement. States may also follow suit with New York, which recently amended its data breach notification law to expand the definition of personal information to include additional data elements. These types of changes provide additional means for state regulators to investigate potentially unlawful activity and pursue enforcement actions to ensure compliance.

Even with the growing number of state privacy laws and the expanding scope of data breach notification requirements, companies can take proactive measures to protect themselves. Measures to prevent a data incident and comply with the regulations remain the best defenses against the growing risk of enforcement actions and penalties. Investments in robust compliance programs can help to mitigate the risk of potential violations and lessen or avoid costs associated with extensive regulatory scrutiny or penalties.

An initial step in the process is to develop comprehensive data privacy policies that align with applicable regulations, ensuring the guidelines are met. Regular audits of data handling processes—such as collection, storage, and processing—are also essential to ensure that practices align with those policies, as well as the applicable laws and regulations.

Additionally, since a significant number of compliance failures and data security incidents arise from human error, having a well-informed workforce that understands privacy obligations and data security best practices is crucial. Therefore, businesses should prioritize employee training and awareness.

Phishing and Business Email Compromises Will Pervade

As noted above, in many business email compromise events, the attacker phishes or socially engineers the victim to grant an unauthorized user to access their email account. That unauthorized user will often use the access to redirect a payment to an account under their control, to propagate more phishing emails to potential victims, or both. These types of attacks have been growing in recent years, and that trend could continue. These incidents are not as splashy as a headline-grabbing data leak on the dark web, or high-profile ransomware attack, but they can lead to financial loss and

trigger notification obligations under state law.

While technical and policy measures such as MFA and voice verification procedures can help to mitigate threats, user vigilance is also a key tool for preventing phishing attacks. A strong awareness and training program that incorporates frequent testing and practicing what to do in the event of an incident can help users stay alert to these types of threats. Moreover, inculcating a culture that encourages users to report suspicious emails and self-report their own interaction with a potential phishing message can help to prevent or reduce the impact of a phishing attack.

AI in the Attacker Toolbox?

AI has become a major topic of discussion in cybersecurity, with many speculating on its potential role in both defensive and offensive strategies. While AI is gaining traction, it continues to be a minor factor in the most common attack techniques today. Current attack strate-

The advertisement for ADR OF COUNSEL features a header with the organization's logo and name. Below this, a dark blue banner reads "EXPERT PANEL MEDIATORS". A grid of ten headshots of mediators is displayed, each with their name underneath. At the bottom center is a QR code labeled "Online Mediation Calendar".

ADR OF COUNSEL Active Litigators Mediating				
EXPERT PANEL MEDIATORS				
 Rehan Alimohammad	 John Charbonnet	 John A. Davis	 Kathryn Green	 Mary Martin
 Claire Parsons	 Charles Peckham	 David Siegel	 Nathan Wesely	 Tariq Zafar
 Online Mediation Calendar				

gies, such as phishing, social engineering, and exploiting known vulnerabilities, still dominate the landscape. Most threat actors rely on traditional tools and methods to execute their campaigns, and AI certainly has the potential to enhance attacks in the future. We anticipate seeing AI-powered chatbots used in social engineering or machine learning algorithms that can help identify vulnerabilities faster and more efficiently than traditional methods. 



Lynn Sessions is a partner at BakerHostetler. Ms. Sessions leads the healthcare privacy and compliance team in the digital assets and data management practice group and serves as national co-lead of the healthcare industry team. She focuses her practice on healthcare privacy and data security, breach response, regulatory defense, and Health Insurance Portability and Accountability Act (HIPAA) compliance.



Kimi Gordy is a partner at BakerHostetler. Ms. Gordy navigates complex cybersecurity and privacy issues for clients across the

healthcare space. She is the firm's Houston digital assets and data management leader. Prior to joining BakerHostetler, she was a federal law clerk in the Southern District of Texas, giving her critical insight into the litigation risk that so often follows a data breach.



Pierce Cox is an associate at BakerHostetler. He focuses his practice on digital risk advisory and cybersecurity,

particularly in the areas of regulatory compliance, fraud investigation, and electronic discovery. He advises clients regarding compliance with data privacy laws, preparing for and reducing exposure

to data privacy threats and mitigating potential losses from data breaches or misuse of information assets.



Jessica S. Johnson is an associate at BakerHostetler. Her practice spans privacy and digital risk and cybersecurity, where she advises clients across various industries regarding compliance with federal, state, and international data security laws. Ms. Johnson guides clients across various industries through data security matters, including coordinating digital forensic investigations, determining breach notification obligations, and responding to regulatory inquiries.

Join the HBA

Not yet a member of the HBA?

JOIN TODAY!

<https://www.hba.org>



QUANTUMSUR
creative ideas for a success story

web design brochures advertising





281.955.2449 ext. 1
leo@quantumsur.com
quantumsur.com



THE NATIONAL ACADEMY OF
DISTINGUISHED NEUTRALS

America's Premier Civil-Trial Mediators & Arbitrators Online



View Bios & Available Dates Calendars for our TX Chapter Members, free at
www.TexasNeutrals.org

Proud ADR Sponsor to the
National Defense & Plaintiff
Bar Associations

dri Lawyers
Representing
Business.™



AMERICAN
ASSOCIATION FOR
JUSTICE
The Association for Trial Lawyers