PUBLICATION

Top Privacy and Cybersecurity Issues to Track In 2024

Authors: Matthew George White, Alexander Frank Koskey, III
January 29, 2024

In recognition of International Privacy Day on January 28, we wanted to share some insights on the top privacy and cybersecurity issues for the new year. Data privacy and cybersecurity will continue to be one of the most critical issues facing companies across all industries and sectors this year. In addition to five new state privacy laws, 2024 is expected to bring not only an amplified number of cyberattacks but also increasingly sophisticated attacks, including using emerging technologies such as artificial intelligence (AI), in what is a quickly and continuously evolving threat landscape.

At the same time, companies must confront new federal, state, and industry regulations that require additional policies and procedures, enhanced proactive security measures and practices, and the disclosure of security incidents to numerous regulators on increasingly short fuses. The following article will highlight several of the key issues and critical considerations that companies must face with a variety of privacy and cybersecurity issues along with recommended best practices to help protect your business and your customers going into the new year.

New State Privacy Legislation

This year will see privacy laws in five states go into effect: Washington, Oregon, Texas, Florida, and Montana.

- **Washington**: On March 31, 2024, the Washington State My Health My Data Act will go into effect. The law focuses exclusively on regulating personal health data that is outside the scope of HIPAA and is not as comprehensive as the privacy laws passed in other states. Nonetheless, organizations that conduct business in Washington State and collect, process, share, or sell consumer health data should assess whether they may be subject to the law's new, expansive compliance requirements. The law also provides consumers with a private right of action, making it just the third state privacy law with such a remedy.

- **Oregon**: The Oregon Consumer Privacy Act goes into effect on July 1, 2024. Businesses are subject to the law if they conduct business in the state and collect or process: (1) the personal data of 100,000 or more Oregon consumers; or (2) the personal data of 25,000 or more Oregon consumers and derive 25 percent or more of its annual gross revenue from selling the personal data. While the Oregon law does include certain data-level and entity-level exemptions, they are more nuanced than the broad exemptions seen in many other state privacy laws.

- **Texas:** The Texas Data Privacy and Security Act will also take effect on July 1, 2024. The scope of the law is unique as there are no volume or revenue thresholds. Rather, the law requires compliance by any entity that conducts business in Texas, produces products or services for Texas consumers, and processes or engages in the sale of personal data. The law includes an exemption for certain small businesses and highly-regulated industries but, overall, is likely to apply to nearly any business that operates in Texas.

- **Florida**: The Florida Digital Bill of Rights will be the third privacy law to become effective on July 1, 2024. The scope of the Digital Bill of Rights is extremely limited and only applies to companies with

$1 billion or more in revenue and where at least 50 percent of its global gross annual revenue is derived from the sale of online advertisements or other narrow criteria. It has been well publicized that the law is aimed at "Big Tech" and contains a number of broad entity-level and data-level exemptions which further reduce the scope of companies that may fall within scope.

- **Montana**: Finally, the Montana Consumer Data Privacy Act will become effective on October 1, 2024. Montana's law is very similar to the comprehensive privacy laws passed in other states and applies to controllers who conduct business in Montana or produce products or services targeted to Montana residents and either control or process the personal data of not less than 50,000 Montana residents or controls or processes the personal data of not less than 25,000 Montana residents, and derives more than 25 percent of its gross revenue from the sale of personal data. Notably, the resident threshold excludes personal data that is controlled or processed solely for the purpose of completing a payment transaction.

We also expect to see several additional states pass comprehensive privacy legislation, such as New Jersey, who recently passed legislation that will go into effect in January 2025.

Evolving Cyber Threat Landscape

The cyber threat landscape will undoubtedly continue to evolve in 2024. The volume of attacks will continue to increase against companies in all industries, regardless of size. This dynamic is underscored by the fact that businesses are continuously incorporating new technologies, gathering increasing volumes of data, storing much of that data digitally, and sharing that data with vendors and service providers. Additionally, while phishing and social engineering threats have not gone anywhere, threat actors are also leveraging emerging technologies such as AI to exploit vulnerabilities. All businesses should be vigilant in detecting and defending against the following:

- **Advanced Social Engineering and Phishing Attacks:** Threat actors are continuing to use phishing and social engineering attacks to target and manipulate employees, including IT help desk representatives, into downloading malware onto company systems and/or disclosing login credentials and other sensitive information. Threat actors are also using generative AI technology to create more convincing phishing email campaigns, and doing so in a variety of languages, making phishing attacks more harmful than ever. Indeed, according to Coveware, phishing and business email compromises represented the initial access method in nearly 25 percent of attacks in the third quarter of 2023. All companies must continue efforts to train employees to avoid these phishing campaigns, and in parallel, should consider new anti-phishing technologies that can help reduce the volume of these attacks. Additionally, companies should implement MFA (multi-factor authentication) wherever possible across their environment, and require complex, frequently changed passwords to limit a threat actor's ability to obtain usable company credentials.

- **Ransomware Attacks**: Threat actors are continuing to evolve their efforts to extort organizations into paying ransoms. It has become commonplace in a ransomware attack for a threat actor to both exfiltrate a company's data and encrypt its systems. However, threat actors have implemented new methods to put pressure on organizations, including hosting "leak sites" where they publish the names (and data) of their victims and sending communications directly to third parties and customers notifying them that their data is at risk with greater frequency. Companies must implement and refine controls to detect and prevent ransomware attacks along with procedures to efficiently respond to such attacks when they occur. Additionally, all companies should assess the location(s) and viability of their backups, test the restoration of those backups, and ensure they have an accurate idea of the time it would take to actually restore from those backups. Further, companies should also be regularly testing their incident response procedures through tabletop exercises to ensure their team is

prepared when an attack happens.

- **Deepfakes + Artificial Intelligence**: Threat actors will continue to build on the use of emerging technologies like artificial intelligence to perpetrate financial fraud and other similar attacks. One particular trend we are seeing is the use of "deepfakes" to create fake images, audio, or videos in an effort to obtain a fraudulent wire transfer. The volume of this type of attack has been increasing, and companies need to ensure they have appropriate policies and procedures in place to prevent such wire fraud from occurring. These need to include sufficient measures to verify the legitimacy of all wire transactions and the validity of all wiring instructions. Additionally, companies need to be prepared to act quickly in the event of a fraudulent wire transfer, as the ability to recover funds decreases exponentially in the hours and days after the transmission.

SEC's Cybersecurity Disclosure Rules

Among many new rules and regulations, one in particular that will be at the forefront of cybersecurity regulatory and compliance for companies in 2024 is the Security and Exchange Commission's (SEC) Cybersecurity Disclosure Rules.

- **SEC's Cybersecurity Disclosure Rules**: The SEC's long-awaited rules went into effect in December 2023 and require public companies to disclose material cybersecurity incidents within four business days of determining an incident is material. The rules further require public companies to disclose, among other things, their processes for assessing, identifying, and managing material risks for cyber threats, as well as the cybersecurity oversight responsibilities of their Board and executive management, in their annual reports. Although planning for these rules has likely been ongoing for several months, publicly traded companies will continue to grapple with these new requirements into 2024. Notably, companies must ensure that processes for identifying and managing cyber risks are in place and procedures for determining materiality are continually assessed and simulated during tabletop exercises. Additionally, companies will need to be prepared for additional regulatory scrutiny and even litigation resulting from these new disclosure requirements. However, the rules will not only affect publicly traded companies. Many private companies who are vendors or service providers of publicly traded entities will be required to provide information concerning their cybersecurity programs to their customers and will likely also meet new contractual obligations being pushed down from their publicly traded customers.

Heightened Class Action Litigation and Regulatory Enforcement Risks

Class action litigants have become increasingly active in the cybersecurity sector. Due in part to additional disclosure requirements under a variety of regulations, there is frequently information made publicly available following a cyberattack. The current trend is that with respect to any of these incidents that result in the disclosure of personal information, class action lawsuits are being filed quickly and in large numbers. This exponential rise in data breach class action litigation is likely to continue into 2024. Companies need to be prepared for such litigation, including ensuring that concepts of the attorney-client privilege are incorporated into the incident response process itself. Moreover, last year saw a litany of enforcement actions against companies by various regulators, resulting in millions of dollars of penalties, around alleged violations relating to improperly stored passwords, failure to manage third-party risk, and a lack of risk assessment policies and procedures. Companies must account for the significant regulatory and legal consequences that may arise after experiencing a security incident or by failing to implement required controls within their compliance programs and their incident response planning efforts.

Vendor Management and Supply Chain Risk

Supply chain attacks dominated headlines last year as threat actors exploited vulnerabilities with critical third-party vendors commonly used by companies. Vendor and supply chain attacks targeted file-sharing software,

password managers, VPN devices, cloud storage providers, and others. On the heels of these attacks, companies must continue to refine third-party risk management procedures. This includes, among other things, identifying critical vendors, understanding the information shared with such vendors, ensuring that third-party vendors have effective controls in place to protect against evolving cyber threats, and monitoring those vendors on a routine basis. Due diligence remains an integral part of this process and companies must perform a comprehensive evaluation of third-party vendors to assess and understand potential risks. It is also more important than ever for companies to have appropriate contract provisions in place to help protect the institution and their customer's information in the event of a data incident, and to ensure that the company is informed throughout the incident response process.

Best Practices for Companies in 2024

2024 is shaping up to be a critical year for companies to prepare themselves to defend against evolving cyber threats. Below are several best practices that companies should implement going into the new year.

- **Evaluate Privacy Practices and Update Privacy Policies:** With five new state privacy laws, companies must evaluate whether they fall within the scope of the new laws and incorporate any new requirements into their privacy policies. Any privacy assessment should also include an evaluation of the company's vendor management program, including additional due diligence requirements and necessary updates to vendor agreements to ensure compliance.

- **Review Incident Response Plan**: A variety of cybersecurity regulations require companies to report cybersecurity incidents to designated regulators and/or have written incident response plans. While having an incident response plan has been a "best practice" for some time, companies should review these plans now to ensure that they incorporate appropriate procedures and controls to protect against new and developing cyber threats.

- **Develop Policies and Procedures to Evaluate Materiality**: Those companies subject to the SEC's Cybersecurity Disclosure Rules (and vendors of those companies) should develop and/or refine policies and procedures to evaluate the "materiality" of a cyber incident. This would include identifying key factors that would make an incident material, the team members involved in assessing materiality, and the requisite chain of communication for relevant information. It is imperative that companies have sound policies and procedures in place to address these requirements.

- **Conduct a Tabletop Exercise**: Companies should also conduct a tabletop exercise to simulate a data incident and test its incident response plan and associated procedures. Notably, any exercise should emphasize scenarios where new regulatory reporting requirements may be at issue and test the responsiveness of the incident response team. Companies must think through these issues during a tabletop exercise in order to be prepared when an actual data incident occurs. Feedback and lessons learned from the tabletop should then be incorporated into the incident response plan, and the process should be repeated at appropriate regular intervals.

- **Assess Vendor Management Protocols**: In addition to incident response policies and procedures, companies should also evaluate existing vendor management protocols to ensure that they appropriately address the increasing risks associated with vendor incidents. Companies should also review due diligence questionnaires to third-party vendors and current "form" master agreements used with third-party vendors and update existing language as needed to implement additional requirements for security controls, incident reporting, and audit capabilities. Current vendor agreements lacking appropriate provisions may also need to be amended.

- **Senior Leadership and Board Engagement**: Engagement by a company's senior leadership team and board of directors on cybersecurity issues is no longer a luxury, it is a necessity. Companies should review and refine processes around how senior leadership is involved in assessing cyber risk and the oversight by the board of directors. Companies would be best served by providing additional education and training to these respective groups so that they are appropriately prepared to address material cyber risks.

Following the suggestions in this alert will help companies prepare themselves to appropriately respond to the litany of new issues they will face this year.

If you have any questions concerning these issues or any aspect of your cybersecurity or privacy programs, please contact the authors Matt White or Alex Koskey, or any member of Baker Donelson's Data Protection, Privacy, and Cybersecurity Team.