Published on *The National Law Review* https://natlawreview.com

5 Trends to Watch: 2023 Data Privacy & Cybersecurity

Article By:

Gretchen A. Ramos

Dr. Viola Bensinger

Jena M. Valdetero

David A. Zetoony

1. **An Increase in Extortion-Only Cyber Attacks** – While ransomware attacks have been on the rise since 2020, a recent trend has emerged where threat actors are bypassing ransomware malware and encryption tactics and going straight to data theft. If a victim company does not pay the extortion demand, the threat actors engage in increasingly aggressive tactics, like publicly posting the stolen data for sale on a shame site and contacting employees and customers of the victim company to apply external pressure on the victim to make the payment.

2. **Continued Increase in Legal Requirements for Company-Held Data –** An increasing number of proposed data security laws and regulations, such as the FTC Safeguards Rule and the EU NIS2 Directive that came into force in 2023, are mandating specific data security measures for companies regulated by those laws, in particular, financial institutions and other highly-regulated industries. These granular laws are leaving behind the more general requirements of the past, which required companies to implement and maintain more vague "reasonable and appropriate" security standards, in favor of requirements that more closely align with recognized data security standards (e.g., NIST, ISO). The laws prescribe not only security measures, but also policies and procedures, incident response plans, and accountability.

3. **Increasing Vendor Due Diligence –** Conducting diligence on vendor data *security* practices has arguably risen to the level of industry standard and practice. Conducting due diligence on vendor data *privacy* practices, including such things as how they handle law enforcement requests, the countries to which they transfer personal information, and their relationships with subprocessors, is less common. Facing increasing scrutiny (and significant fines for breaches) from regulators in the United States and in the European Union regarding the use of processors, controllers are increasingly demanding more information about their vendors' data privacy practices including requesting that vendors substantiate that they have "flowed

down" privacy-related provisions found in their data processing agreements (DPA) to subprocessors. For a guide on how to apply the new European Standard Contractual Clauses to all contracts, see Greenberg Traurig's Complete Handbook for Cross Border Transfers of Personal Information.

4. **Enforcement of California's Privacy Law –**In August 2022, the California Attorney General's office published its first enforcement action and imposed its first fine in relation to an eCommerce website's use of targeted advertising technology. Although enforcement of the California Privacy Rights Act (CPRA) is not permitted until July of 2023, the California Attorney General may attempt to ramp up its enforcement of the California Consumer Privacy Act (CCPA) until that date. After July, it is likely the California Privacy Protection Agency will try to make its mark by initiating enforcement actions and warnings to companies that have not updated their compliance programs to account for the new law.

5. **More Privacy Class Action Litigation Based on Wiretapping Laws** – "Session replay" refers to a tool that records and analyzes customers' interactions with a business's website or phone application to improve functionality and user experience. Over the last few years, a trend has emerged of plaintiffs alleging the use of session replay software violates anti-wiretapping laws which were intended to prevent eavesdropping and secret recordings. It is likely that plaintiffs will continue to assert these arguments in an attempt to impose statutory damages through litigation by shoehorning AdTech tools into violations of wiretapping statutes.

National Law Review, Volumess XIII, Number 26

Source URL:https://natlawreview.com/article/5-trends-to-watch-2023-data-privacy-cybersecurity