Articles + Publications | December 7, 2023

Challenging Recent Developments for Incident Response

Privacy & Cybersecurity Newsletter

WRITTEN BY

Theodore P. Augustinos | Alexander R. Cox | Brianna L. Dally | Lindsey E. Kress | Kenneth K. Suh

RELATED OFFICES

Hartford

The United States is on track to see a record number of data breaches in 2023 and state regulators are paying attention. The swift action required by victim companies includes containment and elimination of the threat, and quick and thorough analysis to determine required notifications to state and Federal agencies, affected individuals, and other third parties. Notice requirements vary by jurisdiction, as does the level of regulatory oversight. The need for companies to strengthen their incident response plans is highlighted by the recent increase in the volume, severity and complexity of incidents, and changes in the legal, regulatory and litigation environment. Good preparation will reduce the time and increase the effectiveness of breach response and help mitigate the related cost and potential exposure.

Increase in Volume, Severity and Complexity

Data breaches show a 17% uptick from 2022 figures.[1] This increase in volume is matched by a continued trend in fewer individuals affected per incident, as in prior years there were more large consumer breaches, but the overall number of events was far lower. For example, 2017 saw 1,506 events affecting 1.8 billion individuals, while 2023 has so far seen 2,116 events with only 234 million individuals affected.[2] This may suggest that threat actors are increasing in sophistication and focusing in on higher value information and targets. One clear hallmark is the prevalence this year of substantial zero-day attacks affecting major back-end information processing companies.

In addition to the increased volume of breaches during 2023, the MOVEit breach represented a severe and complicated breach that involved the records of millions of individuals, and thousands of companies. These companies either used the software compromised by a zero-day vulnerability, or engaged a vendor, sub-vendor or sub-sub-vendor that did. The cases involving vendors and sub-vendors raised issues harkening back to the Blackbaud breach[3] in which more than 13,000 of Blackbaud's customers were affected by a breach of its systems, exposing the customers' data, including personal information of customers in 49 states and the District of Columbia. In MOVEit, the severity was intensified by the magnitude and nature of the affected data. Many of the affected companies (or their vendors) used MOVEit to transfer large volumes of data, including Social Security numbers and other sensitive personal information. Some of the affected vendors had many customer relationships, all or many of which were affected. The nature and complexity of the relationships makes it difficult in many vendor breaches to associate the affected individuals with the relevant companies required to give notice. This difficulty results in delays in notifications, which increase exposure to regulatory action and litigation. With the

recent increase in vendor breaches, the environment presents more risk, cost and exposure.

Changes in the Legal, Regulatory and Litigation Environment

Adding further complexity, cost and exposure, breach notification laws and regulations continue to be adopted and amended to expand the scope of personal information, to set and shorten deadlines for notices, and to impose new notice requirements and specific requirements for ransom payments.

Recently, state breach requirements have expanded to include new forms of personal information, including biometric information, and states continue to add health and medical information.

Perhaps the most notable regulatory change for publicly traded companies is the new SEC rule, which goes into effect on December 18, 2023.[4] The SEC's new rule requires disclosing "material" cybersecurity events on Forms 8-K and 10-K, the former must be made within four days of the determination that the event was "material," a term that has no specific definition. The disclosures must include (1) the material aspects of the nature, scope, and timing of the incident; and (2) the material impact or reasonably likely material impact on the registrant, including on the registrant's financial condition and results of operations.

Industry Specific Regulations

Depending on the state, insurance licensees may have additional requirements to notify insurance and other regulatory agencies, including in New York and states that follow the National Association of Insurance Commissioners ("NAIC") Data Security Model Law. Under the NAIC Model Law, a licensee must notify the state insurance commissioner of a breach within 72 hours of determining that a breach occurred if (i) the forum state is the licensee's state of domicile, or (ii) the licensee reasonably believes that the personal information of 250 or more residents of the forum state were impacted and the licensee is (a) required to give notice to any other agency by state or federal law or (b) there is a reasonable likelihood of material harm to impacted consumers of the forum state or the licensee's business operations.[5]

We can expect more changes, with an amendment to the New York DFS Cybersecurity Regulation (with some new sections effective as soon as December 2023 and other portions coming online over the next two years), which includes new requirements for providing notice of any ransom payments within 24 hours of the payment and in the next 30 days to provide details about why the payment was made.

On the Federal front, the National Credit Union Administration (NCUA)'s issued an amended Cyber Incident Notification Requirements rule that requires notification within 72 hours of an incident "that actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information on an information system or actually or imminently jeopardizes, without lawful authority, an information system."[6] The NCUA's rule includes specific examples of the types of incidents that require notification and notice must be provided through its secure webmail system or to a specific email address.

State attorneys general and other state agencies have gotten more deeply involved in more breaches, signaling a potential increase in the volume of formal enforcement actions. They have clearly devoted more resources to following up on breach notices, to ask additional, sometime very probing questions, concerning the nature and

origin of the incident, the preparedness of the breached entity, and the timeliness and adequacy of the response. It is rare to submit notifications to multiple jurisdictions, and not have regulatory follow up.

Another unfortunate change that increases complexity, cost and exposure is the requirement to submit breach notifications to state agencies on their own, specific webforms. This new process, which has proliferated throughout the attorneys general, and state and Federal regulators, has dramatically increased the cost and time required to complete notifications. We're hopeful that agencies will adopt a common, multi-jurisdictional form to lower the time and expense required to provide notice.

Recent high-profile breaches such as MOVEit have also increasingly drawn the attention of class action lawyers, and this activity is only expected to proliferate as breaches become more publicized through the mainstream media and through regulatory agencies.

The landscape of incident response has changed. While headlines and media attention will be focused on big-high-visibility incidents, the real fight is now in the targeted attack. Companies face an increasingly complex web of reporting requirements in addition to the evolving technical challenge of information security. Sectoral regulators are likely to continue the trends seen in insurance and financial industries and we expect more industry specific rules to roll out across various jurisdictions. This balkanization of reporting requirements is unlikely to be solved by comprehensive federal action, but companies are better served than ever by investing in incident response planning to both understand the technical response to an incident and to prepare for the potential legal challenges here and on the horizon.

—

[1] ID Theft Resource Center, *Q3 2023 Data Breach Report: Identity Theft Resource Center Reports Data Compromise Record with Three Months Left in the Year* (Oct. 11, 2023), https://www.idtheftcenter.org/post/q3-2023-data-breach-report-itrc-reports-data-compromise-record-with-three-months-left-in-year/

[2] *Id.*

[3] SEC.Gov, *SEC Charges Software Company Blackbaud Inc. for Misleading Disclosures About Ransomware Attack That Impacted Charitable Donors* (Mar. 9, 2023), https://www.sec.gov/news/press-release/2023-48; Bloomberg Law, *Blackbaud Resolves Multi-State Attorneys General Investigation of 2020 Security Incident* (Oct. 5, 2023),

https://news.bloomberglaw.com/privacy-and-data-security/blackbaud-settles-data-breach-with-49-states-dc-for-50-million

[4] Smaller Reporting Companies have a 180-day deferral period

[5] E.g., 23 NYCRR 500; S.C. Code of Laws §§ 38-99-10 to 38-99-100 ; CGS §38a-38; KY HB 474; Miss. Code §§ 83-5-801 to 83-5-825; MD SB 207

[6] https://ncua.gov/regulation-supervision/letters-credit-unions-other-guidance/cyber-incident-notification-requirements

RELATED INDUSTRIES + PRACTICES

- Incidents + Investigations
- Privacy + Cyber