Consumer & Commercial Law State Bar of Texas

The Breach Is Over: The Defense Costs Are Just Beginning

Blog Hunton Insurance Recovery Blog

Hunton Andrews Kurth LLP

USA | September 3 2026

When a cyberattack occurs, companies often focus on the immediate response—investigating the breach, restoring systems, notifying affected individuals, and managing business disruption. But those costs are often only the beginning. In the months and years that follow, organizations increasingly face class actions, regulatory proceedings, and other claims alleging that they failed to safeguard sensitive information, and the cost of defending those actions can ultimately exceed the cost of responding to the breach itself.

The litigation arising from Novo Nordisk's recent cyber incident illustrates this point. According to the complaint, cybercriminals allegedly obtained access to the company's systems and exfiltrated approximately 1.3 terabytes of data and roughly 700,000 files. The plaintiff alleges negligence, negligence per se, breach of implied contract, and unjust enrichment, and seeks damages, injunctive relief, attorneys' fees, and other relief on behalf of a proposed nationwide class.

The Real Cost of a Cyberattack Often Begins After the Breach

The Novo Nordisk lawsuit highlights a reality that many policyholders may overlook: the most significant financial exposure from a cyber incident is often not the breach itself, but the litigation that follows. The complaint alleges that Novo Nordisk failed to implement reasonable cybersecurity safeguards, failed to comply with accepted industry standards, and failed to adequately protect sensitive information entrusted to it. The plaintiff seeks damages based on, among other things, the alleged risk of identity theft, time spent monitoring accounts, emotional distress, and the loss of the value and privacy of personal information.

From an insurance perspective, however, the ultimate merits of those allegations are often not the most important issue. Even where liability is disputed and no wrongdoing has been established, a data breach can quickly evolve into expensive third-party litigation. Companies may face class actions, privacy claims, and regulatory investigations that require years of motion practice, discovery, expert analysis, and settlement negotiations. The cost of defending those proceedings can be substantial regardless of the ultimate outcome.

This is where cyber insurance often provides its greatest value. In addition to providing coverage for first-party expenses, cyber policies generally contain liability coverage designed to respond when third parties assert claims arising out of a cyber incident. Depending on the policy language, a lawsuit alleging that the insured failed to protect confidential information, maintain adequate network security, or comply with privacy obligations may constitute a covered claim. Likewise, many policies contemplate coverage for regulatory proceedings and investigations arising out of an alleged privacy or security failure.

As a practical matter, that means a cyber policy may provide coverage not only for investigating and responding to a breach, but also for the legal fees incurred in defending the litigation that follows and, in some circumstances, the amounts paid to resolve those claims. Yet the policy terms governing the defense of claims can become just as important as the coverage grant itself. Once litigation begins, questions regarding who controls the defense, when costs may be incurred, and how policy limits may be affected can significantly influence the value of the coverage available.

Coverage Issues That Arise After the Complaint Is Filed

Ideally during the renewal process, and certainly once litigation begins, policyholders should pay close attention to the provisions governing the defense of claims. Defense-cost erosion, insurer-consent requirements, reporting obligations, and control-of-defense provisions can materially affect both the value of the coverage purchased and the handling of the litigation itself. These provisions influence not only how claims are funded, but also who makes strategic decisions, how counsel is selected, when settlements may be pursued, and whether the interests of the insurer and policyholder remain aligned throughout the litigation.

Accordingly, policyholders should consider the following issues when evaluating how their cyber policies will respond to a claim.

1. **Defense costs may erode available limits**. Many cyber policies provide that defense costs reduce the policy's limits of liability. As a result, a policyholder facing years of class-action litigation may find that a substantial portion of its insurance has already been consumed by attorneys' fees, expert costs, and discovery expenses before settlement discussions even begin.
2. **Consent provisions can become critical**. Many cyber policies require the insurer's consent before defense costs are incurred or settlements are reached. Failure to obtain that consent can later result in disputes regarding reimbursement of defense expenses or settlement amounts.
3. **Control of the defense matters**. Even where coverage is available, disputes can arise regarding who controls the defense and how the litigation will be managed. Policies differ on whether the insurer may appoint counsel, require the use of panel counsel, permit the policyholder to select its own defense team, limit reimbursable attorney rates, and influence litigation strategy and staffing decisions. In a complex data-breach case, disagreements over defense strategy, staffing, or settlement can quickly create tension between the insurer and policyholder, making these provisions particularly important. Policyholders should therefore understand these provisions before a claim arises and address potential conflicts with the insurer early.

Takeaways

The Novo Nordisk lawsuit serves as a reminder that the financial consequences of a cyber incident often extend well beyond the immediate costs of responding to the breach. While a cyberattack may last days or weeks, the resulting litigation, regulatory proceedings, and defense costs can continue for years.

When evaluating cyber coverage, policyholders should consider:

1. **Whether the policy provides meaningful protection against third-party litigation and regulatory proceedings.** Many policyholders focus on forensic investigations, notification expenses, and business interruption coverage. But cyber policies frequently provide valuable protection against the claims and proceedings that arise after the breach.
2. **Whether policy limits are sufficient to address years of defense costs, settlement exposure, and related proceedings following a cyber event.** A cyber event can trigger years of litigation and related expenses that may substantially exceed the costs incurred during the initial response.

3. **Whether key defense-related provisions align with the policyholder's expectations.** Policyholders should understand how their policies address defense-cost erosion, insurer consent, and control of the defense before a claim arises.
4. **Whether renewal provides an opportunity to strengthen coverage.** When renewing cyber coverage, policyholders should evaluate policy limits, liability coverage, defense-cost provisions, and other terms that may become critical if litigation follows a cyber event. Renewal often presents the best opportunity to negotiate policy terms before a claim arises and the parties' interests diverge.

Ultimately, policyholders should not view cyber insurance solely as a tool for responding to a breach. In many cases, its greatest value may lie in funding the years of litigation that follow. As cyber litigation continues to grow, policyholders should work closely with experienced coverage counsel to evaluate their policies, preserve coverage, and maximize available insurance when a claim arises.

Hunton Andrews Kurth LLP - Kevin V. Small and Torrye Zullo