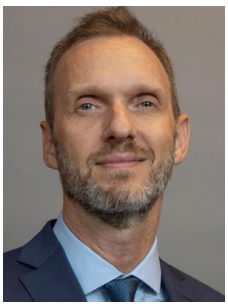
Portfolio Media. Inc. | 230 Park Avenue, 7th Floor | New York, NY 10169 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

5 Critical Factors Driving Settlement Values In Cyber Litigation

By **Peter Kamminga** (June 20, 2024, 5:21 PM EDT)


Peter Kamminga

Recent reports on ransomware attacks highlight cyber incidents' dual financial burden: direct costs and subsequent legal expenses.

The latest example is a May 9 ransomware attack on Ascension Health, one of the largest health systems in the country, facing a proposed class action only days after being attacked.[1]

This article delves into recent cases to uncover the critical factors driving the settlement value of legal claims resulting from cyberattacks.

Cyber Incidents and Their Consequences

Last year was a record year for ransomware gangs, with crypto ransom payments doubling to exceed $1 billion for the first time.[2] The impact of ransomware extends across various industries, with the healthcare sector alone projected to spend $125 billion on breach defenses from 2020 to 2025.

This year has seen a resurgence in attacks on high-value targets — so-called big game hunting — while smaller organizations, including law firms, also face escalating data breach costs.[3]

The evolution of attack methods, particularly those leveraging AI for more sophisticated social engineering, poses a growing challenge for detection and prevention.

Simultaneously, regulatory environments are tightening, with stricter incident reporting and compliance requirements coming into play.[4]

Litigation Risks in Data Breach Incidents

Organizations that have experienced a data breach face substantial litigation risk in various areas, including regulatory enforcement actions and fines, data privacy claims — often class actions — contractual disputes and disputes with insurers over cyber incident coverage.

Hackers not only encrypt data but also steal it. A recent ransomware report surveying organizations that fell victims of cyberattacks in 2023 concluded that 32% of the reported incidents where data was encrypted, it was also stolen.[5]

In fact, data theft enhances attackers' ability to extort money from their victims and allows them to further monetize the attack by selling the stolen data on the dark web.

A cyber incident can trigger claims for alleged failing to maintain adequate cybersecurity measures, inadequately protecting sensitive information and not issuing breach notifications in a timely manner.[6] Organizations can also be sued for making false and misleading statements and concealing vulnerabilities.

Organizations that fall victim to a data breach and make the news inevitably encounter legal challenges, but the extent of bad behavior — such as failure to adequately protect sensitive information — can significantly influence settlement values. Recent substantial regulatory fines for data breaches indicate growing regulatory rigor in protecting consumer data.

Despite the U.S. Supreme Court's 2021 TransUnion v. Ramirez decision,[7] which led to stricter requirements for plaintiffs to claim standing based on the risk of future harm, some lower courts have allowed these claims to proceed if the risk has resulted in tangible injury.[8]

Understanding these litigation risks underscores the need for robust cybersecurity practices, timely breach reporting and transparent communication to minimize potential legal fallout and settlement costs.

Notable Cases Highlighting Cyberattack Trends

The impact and fallout of cyberattacks can be illustrated with some recent high-profile examples:

UnitedHealth Group

A ransomware attack on UnitedHealth Group Inc. in the first fiscal quarter of 2024 led to the theft of private healthcare data, several ransomware demands and a $22 million ransom payment, with an overall reported loss of $872 million. This breach illustrates the severe financial and privacy consequences of ransomware attacks in the healthcare sector.[9]

Fujitsu

Fujitsu Limited suffered a significant cyberattack, also in the first fiscal quarter of 2024, highlighting the global reach and impact of cyberthreats on essential IT service providers.

Caesars Entertainment

A ransomware attack on Caesars Entertainment Inc. led to a reported ransom payment of $15 million in the third fiscal quarter of 2023. This case highlights the potential rapid escalation of ransomware attacks and the financial pressures organizations face to resolve such incidents swiftly. The incident was quickly followed by a proposed data breach class action.

MGM Resorts

A ransomware attack on MGM Resorts lasted 10 days in the third fiscal quarter of 2023, which cost the company an estimated $110 million. This incident exemplifies the substantial operational and financial impact prolonged cyberattacks can have on major enterprises. Class actions were brought.

Microsoft

Hackers obtained keys to Microsoft Corp.'s email systems in the third fiscal quarter of 2023, granting near-unfettered access to U.S. government email accounts. This breach underscores the critical importance of securing email infrastructure.

MOVEit

The MOVEit software was compromised in the second fiscal quarter of 2023, affecting over 60 million individuals. This incident highlights the risks associated with widely used third-party software and the broad impact a vulnerability in the software can have. It triggered claims against the company and against organizations using the software.[10]

Uber

An 18-year-old hacker accessed Uber Technologies Inc.'s systems in the third fiscal quarter of 2022 through stolen employee credentials, gaining full administrative access. This breach underscores the vulnerabilities associated with social engineering and the importance of robust credential management. Uber has been hacked multiple times in recent years.[11]

SolarWinds

In the last fiscal quarter of 2019 and the first fiscal quarter of 2020, hackers embedded malicious code into SolarWinds Corp.'s Orion IT monitoring software, affecting thousands of enterprises and government agencies globally.

The U.S. Securities and Exchange Commission sued SolarWinds and its chief information security officer for allegedly concealing poor cybersecurity practices. This case underscores the regulatory and reputational repercussions of an extensive cyber breach.

5 Settlement Value Drivers

These recent ransomware incidents and their legal repercussions offer valuable insights into the determinants of settlement values in cyberattack-related litigation. Understanding these trends and their implications can better prepare organizations for the potential legal fallout from future breaches. Five settlement value drivers stand out, as discussed below.

1. The Decision Regarding Paying Ransom

The decision to pay or not to pay a ransom can affect the settlement value of legal claims following a ransomware attack. Paying the ransom can protect sensitive information but may violate U.S. federal regulations and does not guarantee data recovery.

Refusing to pay avoids regulatory risks, but may lead to higher immediate costs. A recent survey indicates that organizations often adopt a wait-and-see approach, evaluating each incident's specifics before deciding whether to pay. Establishing a clear ransomware policy expedites decision making during an attack.

2. The Role of Cybersecurity Awareness in Legal Outcomes

The cybersecurity culture within an organization significantly affects the settlement value of legal claims following a cyberattack.

A company's commitment to cybersecurity is reflected in its training programs, awareness initiatives and overall preparedness. Organizations that fail to evolve their training and awareness programs are at a higher risk of incurring significant settlement costs.

Investing in advanced cybersecurity training and engaging in regular exercises can mitigate the impact of a breach and influence perceived responsibility and negligence in legal claims, particularly if this culture also extends to vendors and their cybersecurity measures.

3. The Impact of Reporting Timeliness

The time a company takes to report a cyber incident can significantly affect the settlement value of legal claims arising from a breach. Quick reporting demonstrates an organization's commitment to transparency and responsibility, potentially limiting the damage.

Timely disclosure allows affected parties to take protective measures and portrays the organization as caring and open. Failure to report promptly can exacerbate the consequences of a breach and increase the settlement value of related claims.

Recent regulatory developments emphasize the importance of prompt reporting. Public companies are required to disclose material cybersecurity incidents promptly. Delayed reporting can lead to accusations of concealment and regulatory noncompliance, significantly increasing the settlement value of claims.

4. The Impact of Hack History

Having a history of cyberattacks can affect the settlement value of legal claims arising from subsequent breaches. Organizations with a history of breaches are scrutinized more intensely and expected to demonstrate substantial improvements.

The rapidly changing legal landscape demands quick compliance and adaptation. Failure to meet these heightened expectations can lead to increased settlement values due to perceived negligence and inadequate cybersecurity practices.

Regular audits help identify strengths and weaknesses in security measures. A risk-focused strategy involves identifying critical risks and working backwards to ensure compliance while securing vital assets.

5. The Role of Cyber Insurance in Legal Settlements

The presence or absence of cyber insurance can also influence the settlement value of legal claims following a cyberattack. Having insurance is a sign a company is taking cybersecurity serious and also maintains a sufficient level of protection to obtain it.

Cyber insurance provides a financial safety net and offers a risk management support that can help limit

the fallout, get systems back on track and negotiate down ransoms.

Acquiring and maintaining cyber insurance involves meeting stringent criteria, including comprehensive cybersecurity protocols and a detailed application process.

Coverage affects the settlement process by determining available financial support, although policies have limitations, as seen in the Merck & Co. Inc. case. A $1.4 billion claim was denied based on hostile action exclusions, but was eventually settled by the parties in New Jersey Supreme Court in January.[12]

Key Takeaways on Drivers of Settlement Value

Understanding and anticipating the factors that drive settlement values in cyber incident-related or data breach litigation is crucial to make informed choices related to cybersecurity measures and minimize legal fallout:

- Prevention: Ensure robust and up-to-date cybersecurity measures to mitigate potential breaches effectively.
- Preparation: Have and follow incident protocols to handle breaches and minimize damage.
- Response: Act quickly to mitigate risks and adhere to established protocols.
- History: Demonstrate substantial improvements in cybersecurity practices following a previous breach.
- Information sharing: Communicate transparently and swiftly about incidents to manage reputational damage and regulatory compliance.
- Awareness: Ensure leadership is informed and proactive in addressing potential vulnerabilities.

The landscape of data breach litigation is complex and multifaceted. By understanding and addressing the key drivers of settlement values, companies can better navigate the legal and financial challenges of cyberattacks.

A proactive and comprehensive approach to cybersecurity minimizes potential legal fallout and enhances the organization's overall resilience and reputation.

Peter Kamminga is a mediator at JAMS.

[1] Ascension Health Data Breach Lawsuit Filed After May 2024 Cyberattack Affecting MyChart Portal, classaction.org, May 15, 2024: https://www.classaction.org/news/ascension-health-data-breach-lawsuit-filed-after-may-2024-cyberattack-affecting-mychart-portal.

[2] Cyber gangs got away with a record $1.1 billion in crypto ransom payments in 2023, Business Insider,

February 7, 2024: https://markets.businessinsider.com/news/currencies/crypto-cyber-crimes-ransom-payments-record-hacks-ransomware-2023-2024-2?op=1.

[3] "Cost of a Data Breach Report 2023," IBM Security, July 25, 2023, https://www.ibm.com/reports/data-breach.

[4] SEC breach report and disclosure requirements 2023, July 26, 2023: https://www.sec.gov/files/rules/final/2023/33-11216.pdf and CISA Cyber Incident Reporting rule, April 4, 2024: https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/cyber-incident-reporting-critical-infrastructure-act-2022-circia.

[5] The State of Ransomware, 2024, Sophos, April 30, 2024: https://news.sophos.com/en-us/2024/04/30/the-state-of-ransomware-2024/.

[6] NYSE Exchange Owner Fined $10 Million Over Breach Reporting Failure, May 28, 2024, https://www.cpomagazine.com/cyber-security/nyse-exchange-owner-fined-10-million-over-breach-reporting-failure/.

[7] TransUnion v. Ramirez , 594 U.S. at 435-36: https://supreme.justia.com/cases/federal/us/594/20-297/.

[8] Webb v. Injured Workers Pharm. , 72 F.4th at 376: https://casetext.com/case/webb-v-injured-workers-pharm and Bohnak v. Marsh&McLennan Cos. , 79 F.4th at 286: https://casetext.com/case/bohnak-v-marsh-mclennan-cos-2?.

[9] Zack Whittaker, "UnitedHealth says Change hackers stole health data on 'substantial proportion of people in America,'" TechCrunch, April 22, 2024.

[10] Kelly Mehorter, "Columbia University Hit with Class Action Over MOVEit Data Breach," classaction.org, November 28, 2023: https://www.classaction.org/news/columbia-university-hit-with-class-action-over-moveit-data-breach.

[11] "Uber Investigating Breach of Its Computer Systems," New York Times, September 2022.

[12] Carrie Pallardy, "Merck's Cyberattack Settlement: What Does it Mean for Cyber Insurance Coverage," Information Week, Jan. 12, 2024.