Policyholder Best Practices As Cyberattacks Escalate

Law360

September 4, 2021

Lee Epstein & Krishna Jani, CIPP/US

Cyberattacks are exploding. The coronavirus pandemic has further exposed cyber vulnerabilities due to remote work and the increasing use of underprotected devices. Ransomware attacks are increasingly becoming the cyberattack of choice.

While data breach and privacy claims fell between 2018 and 2020, ransomware attacks rose by 486% over that same period. Victims of ransomware paid $350 million in 2020, an increase of 311% over the previous year.

The average ransomware payment in 2020 was $312,943. The costs of ransomware extend well beyond the ransom payments. The average downtime due to an attack is 21 days and it takes a business an average of 287 days to recover.

This explosion of cyberattacks has resulted in greater regulatory oversight and a hard insurance market. As the responses to escalating cyberattacks continue to unfold, corporate policyholders may wish to employ some best practices to avoid regulatory hot water and the worst effects of a hard insurance market.

Heightened Cyber Regulations

Regulators, both nationally and internationally, have sharpened their focus on the privacy rights of individuals and on the regulation of data collection and protection. Regulators are enforcing their regulations through the imposition of fines and the extraction of settlements for noncompliance.

Internationally, the European Union stepped up enforcement of the General Data Protection Regulation. In the first 10 months of 2020, 220 fines were issued, reflecting a 260% increase over the previous year.

Nationally, the second largest Health Insurance Portability and Accountability Act settlement ever was reached in 2020, with Premera Blue Cross agreeing to pay $6.85 million to the U.S. Department of Health and Human Services' Office for Civil Rights.

Also last year, the U.S. Department of the Treasury's Office of Foreign Assets Control issued an advisory stating that ransom payments to cybercriminals that are subject to OFAC sanctions may violate OFAC regulations and result in civil penalties. That advisory clarified that it applied to companies involved in providing cyber insurance, digital forensics investigators, incident response firms, and financial services companies that facilitate the processing of ransom payments.

On the state level, several states, including Illinois, Washington, Texas and Arkansas, have either enacted or amended privacy laws related to the collection, use, and retention of biometric data, resulting in related litigation, including a $650 million settlement involving a class of Illinois residents in In re: Facebook Biometric Information Privacy Litigation.

In addition, several states have proposed and enacted legislation following the California Consumer Privacy Act, aimed at granting U.S. citizens greater control over their personal data.

New York has taken a leading role in cybersecurity regulation directed specifically at insurance companies and other financial institutions. New York's regulation became effective on March 1, 2017, with a two-year

implementation period.

By March 1, 2019, all insurance companies and other financial services institutions and licensees regulated by New York's Department of Financial Services were required to have a robust cybersecurity program in place designed to protect consumers' private data.

In addition, those entities were required to have a written policy or policies approved by the board of directors or a senior officer; a chief information security officer to help protect data and systems; and controls and plans in place to help ensure the safety and soundness of New York's financial services industry including encryption and multifactor authentication.

As many financial institutions are headquartered in or conduct substantial business in New York, this new regulation is significant and may influence how other states decide to regulate cybersecurity.

Cyber Insurance

Cyber insurance has become a standard part of corporate cyber risk management. As cyber losses generally, and ransomware attacks specifically, have increased, a number of insurers have exited the field, and it appears as if cyber insurance has entered a hard market.

A hard insurance market is typically associated with rising premiums and coverage restrictions. Premium increases of between 15%-50% were anticipated for this year. With regard to coverage, insurers are actively evaluating the following coverage terms and conditions.

Ransomware Coverage

In response to the rapid rise in ransomware attacks, insurers are capping aggregate limits and insisting on sublimits. When critical internal controls are lacking, insurers are proposing to exclude ransomware attacks in their entirety.

Contingent Business Interruption

SolarWinds Corp. is a major software company that provides tools for network and infrastructure monitoring, including an IT monitoring system called Orion. More than 30,000 organizations use the Orion system. Following the SolarWinds cyber breach last spring, the hackers were able to gain access to the computer systems of thousands of the company's customers.

The SolarWinds attack prompted insurers to review their overall exposure to contingent business interruption exemplified by supply chain risks exposed by the attack. Specifically, insurers are insisting on greater waiting periods before coverage incepts and reduced aggregate limits and sublimits.

Notice Requirements

Late notice is one of the most common causes of insurance claim disputes under errors and omissions insurance policies. Often those disputes have their origins in the sometimes confusing use of "claims made," "claims made and reported" and "occurrence" notice language. Insureds must pay careful attention to these provisions to ensure proper and timely notice of any cyber loss.

Breach Response Vendors

The costs of responding to a cyberattack, including IT forensics, external services and other specialists, are typically covered under cyber insurance policies. To reduce, or at least stem, the increase in these costs, insurers are becoming increasingly less flexible in the use of nonpanel or preagreed vendors.

Corporate Policyholder Best Practices

Corporate policyholders can proactively employ the following practices to best respond to the heightened regulatory scrutiny and a hardening insurance market.

Enhance Cybersecurity

While cybersecurity risks cannot be eliminated, certain proactive steps can be taken to reduce those risks. Those steps include: the implementation of risk management strategies involving assessment, testing and

practice improvement, incident response preparedness through retention of incident response vendors and incident response practice.

Make Privacy a Focus

Establish and update corporate policies that address third-party contracts, online presence, service providers and supply chains. For example, policyholders may want to ensure that their vendor contracts include the maintenance of requisite privacy and security standards as well as breach notification procedures.

Embrace Cybersecurity Culture

Train employees to spot malicious actors and reduce common cybersecurity and phishing vulnerabilities. Using multifactor authentication and strong passwords can be crucial to staving off threat actors.

Demonstrate Ransomware Preparedness

Develop plans for business continuity, disaster recovery, privileged access controls, multifactor authentication, proactive scanning and testing, and overall incident response readiness. Segregate and test backups to ensure that critical systems can be restored in the face of an attack and put in place a ransomware-specific incident response plan that is tested by senior leadership.

Be Transparent and Communicate

Don't wait for a claim. Be open about potential vulnerabilities and include insurers in your planning. Maintaining open lines of communication with all lines of insurers before a claim arises will enhance outcomes after a claim is presented.

Update: This article has been updated with a citation including an estimate from SolarWinds regarding the scope of the cyber breach last spring. The time frame for the breach in 2020 was also clarified.

Lee Epstein is a shareholder and chair of the insurance counseling and recovery practice group at Flaster Greenberg PC. He represents corporate and individual policyholders in recovering insurance in response to an array of hazards and catastrophic property and business interruption losses. He advises market leaders in the airline, chemical, construction, financial services, food, HVAC&R, packaging, retail and satellite television industries. Lee is currently litigating insurance coverage disputes throughout the state and federal courts of the United States.

Krishna A. Jani, CIPP/US, is a member of Flaster Greenberg's Litigation Department focusing her practice on complex commercial litigation. She is also a member of the firm's cybersecurity and data privacy law practice groups through which she advises clients on matters related to regulatory compliance, data breach response, and crafting privacy-by-design policies.

[1] See Aon-errors-and-omissions-cyber-insurance-snapshot.pdf.

[2] Chainalysis Team, Ransomware Skyrocketed in 2020, But There May Be Fewer Culprits than You Think, excerpt from the Chainalysis 2021 Crypto Crime Report (Jan. 26, 2021).

[3] Unit 42, Palo Alto Networks, Ransomware Threat Assessments: A Companion to the 2021 Unit 42 Ransomware Threat Report, (Mar. 17, 2021), https://unit42.paloaltonetworks.com/ransomware-threat-assessments (last visited Aug. 12. 2021).

[4] Coveware, Ransomware Payments Fall as Fewer Companies Pay Data Exfiltration Extortion Demands, (Feb. 1, 2021), https://www.coveware.com/blog/ransomware-marketplace-report-q4-2020 (last visited Aug.

12. 2021).
[5] Naveen Goud, Ransomware attacks could have cost the United States $7.5 Billion, by Naveen Goud, Cybersecurity Insiders, https://www.cybersecurity-insiders.com/ransomware-attacks-could-have-cost-the-united-states-7-5-billion/ (last visited Aug. 12. 2021).
[6] See Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments, Department of the Treasury, October 1, 2020, ofac_ransomware_advisory_10012020_1.pdf (treasury.gov).
[7] See Facebook Wins Preliminary Approval for Biometric Privacy Accord, Joe Schneider, August 19, 2020, https://news.bloomberglaw.com/privacy-and-data-security/facebook-wins-preliminary-approval-for-biometric-privacy-accor (last visited Aug. 23, 2021).
[8] See 23 N.Y.C.R.R. 500.
[9] See, e.g., "Aon's E&O | Cyber Insurance Snapshot," https://www.aon.com/cyber-solutions/wp-content/uploads/Aon-errors-and-omissions-cyber-insurance-snapshot.pdf; "Cyber another soft market: Gallagher Re," Intelligent Insurer, April 14, 2021, https://www.intelligentinsurer.com/news/cyber-may-never-experience-another-soft-market-gallagher-re-25350 ; 2021 Cyber Insurance Market Conditions Report, https://www.ajg.com/us/news-and-insights/2021/jan/2021-cyber-insurance-market-report/ (last visited Aug. 12. 2021).
[10] On May 7, 2021, in an update about an ongoing investigation, SolarWinds estimated the actual number of customers hacked to be fewer than 100.

ATTORNEYS MENTIONED

Lee Epstein