CRC Group

INSURETrust

Cyber Insurance Remains Critical as Ransomware Attacks Rise

Ransomware groups are continuing their costly attacks on businesses and increasingly turning to double and triple extortion threats as fewer victims are paying the ransom. Increased resilience and heightened vigilance are more important than ever as breach costs soar, rising to as much as an estimated $2.45 billion in a single attack earlier this year.[4 5] As expenses rise, the proper insurance coverage can provide a crucial backstop as well as aid in recovery and help mitigate lasting reputational damage. The complexity and variety of cyber policies, however, deems it crucial to work with knowledgeable brokers who can identify the differences and ensure that clients obtain optimal coverage, including bespoke solutions where appropriate.

RANSOMWARE BECOMES BIG BUSINESS

After declining at the start of the Russia-Ukraine conflict two years ago, ransomware attacks have picked up pace. Major attacks in 2024 have potentially impacted hundreds of millions of people, disrupted auto sales nationwide, and highlighted a significant increase in ransomware exploits overall.

Q1 2024 saw a 21% increase over Q1 2023, and is the most active first quarter ever recorded on ransomware leak sites.[1]

Increasingly, cyber criminals are demanding ransom not only to decrypt networks but to prevent the sale or posting of stolen information and forestall follow-on attacks against a victim's vendors or customers in what are known as double and triple extortion threats. Cyber criminals are constantly changing their techniques to stay ahead of defenses used by organizations. Some ransomware gangs are now offering ransomware as a service to others, making it easier than ever to get access to the technology needed to carry out attacks. In addition to the damage caused by threat actors, organizations face a growing risk of third-party class action lawsuits and regulatory investigations that add a potentially costly long-tail element to cyber claims.

The global reach of ransomware gangs was highlighted in May 2024 when hackers attempted to sell stolen information of more than 500 million users of a leading ticket site on the dark web.[2 3]

That breach followed a ransomware attack earlier this year that caused disruption of hospital and medical services across the U.S. as it targeted a company that handles approximately 33% of American medical records. In July, UnitedHealth Group increased estimates of the total impact for that attack against its Change Healthcare subsidiary to as much as $2.45 billion[4] (from an earlier $1.6 billion estimate) for all of 2024 and acknowledged that it had paid a $22 million ransom in the attack that targeted a portal lacking multi-factor authentication. [5] [6]

A June attack against a software supplier to around 15,000 auto dealers across North American caused widespread disruption, which could cost U.S. dealers more than $1 billion.[7] It was reported that the firm likely paid a $25 million ransom to a hacking group.[8]

Healthcare data breaches are among the most expensive, costing nearly $11M on average in 2023.[9]

FEWER PAY RANSOM

Ransom payments can easily reach into the millions of dollars. For instance, the total ransom paid from an attack that affected users of the MOVEit file transfer software likely reached as high as $100 million.[10] More than 2,500 organizations were victims of that 2023 breach that exposed data of more than 64 million individuals.[11]

Victim organizations are, however, increasingly less likely to pay ransom for decryption keys as companies have invested in, and strengthened, their capabilities to restore and rebuild networks after attacks. There is also an increasing possibility the decryption key may not fully work, if purchased. An estimated record low of 28% of victims paid ransom in the first quarter of 2024, and the average ransom payment dropped by half to nearly $382,000 from the fourth quarter of 2023.[12] Additionally, there has been a shift to companies paying to keep data from being sold, or what is called data suppression. In these circumstances, the victims must remain wary about whether their data will actually be deleted by criminal gangs, as investigations have found that data is not always fully erased.

Meanwhile, law enforcement has achieved some major successes against ransomware gangs. U.S., UK, and international law enforcement bodies announced in February 2024 that they had disrupted the LockBit ransomware group, which had taken more than $120 million in ransom payments while targeting more than 2,000 victims.[13] The U.S. Justice Department announced in December that it had also disrupted the ALPHV/Blackcat ransomware-as-a-service group[14], although they returned to carry out the attack on Change Healthcare before disappearing in March of 2024. However, new groups continue to emerge, and established groups reorganize.

63% of ransom demands are $1 million or more, while 30% of demands are for over $5 million.[15]

RESPONSE COSTS CLIMB

Successful attacks not only cause severe disruption and potentially lasting reputational damage, but also force businesses to bear the high costs to rebuild networks. Even attacks against companies that aren't household names can cause widespread disruption. That risk was highlighted by this year's attack against Change Healthcare and the 2021 attack that forced the temporary closure of a key U.S. gasoline pipeline.[15]

Post-breach costs include data mining to identify exposed sensitive information, which can be material and complex depending on the size of the company and its business. When combined with the expense to rebuild the network, notify the individuals whose information was compromised, and offer protective services such as credit monitoring, the cost to respond to an incident is continuing to climb. Costs can be contained if companies are confident that they've eradicated the malware and wiped and restored their networks. But clients who cannot do so, may have to build an entirely new and clean version of their network, which is a significant technology spend. Aiding efforts to spend less money in the wake of an attack, there are new technologies and vendors seeking to tackle the rising costs of data mining by simplifying the process and even using artificial intelligence in lieu of humans to do the work. And as events in July 2024 showed the industry, significant outages, costs to rebuild, and business interruption claims can arise even from failed patch installation rather than a nefarious attack on the network.

With those costs in mind, companies are generally strengthening how they store and protect their data, which significantly improves their ability to respond and recover. That includes tools and techniques such as endpoint detection and response (EDR, MDR, XDR) technologies as well as segmented and protected backups. Multifactor authentication (MFA) has proven effective, although criminals continue to seek ways around it and hunt for entry points where it is not active. Human error remains a key vulnerability as many breaches are facilitated by phishing attempts to obtain administrator credentials to mount a more potent attack.

Almost 1 in 5 ransomware attacks led to a lawsuit in 2023.[16]

CLASS ACTIONS AHEAD

Third-party liability is becoming a bigger exposure, creating long tail risk. Cyber has been a relatively short-tail coverage and most of the costs—ransom, forensics, breach response, notification costs, and network rebuild—are known within the first six months, potentially 12 months for more complex claims. Increasingly, cyber breaches are being followed by lengthy and expensive litigation involving the violation of privacy laws. Capital One, for instance, agreed in 2022 to a $190 million class action settlement over a 2019 data breach in which the attacker gained access to the personal information of about 98 million U.S. consumers. [16] [17]

Plaintiffs' attorneys are increasingly relying on the combination of privacy law violations and significant classes of affected individuals. Much of this litigation is being settled early as the cases can be expensive to defend, potentially reaching policy limits, and center on the established fact of the exposure of private information. With liability not disputed, the argument centers on the potential award of damages for the threat of future harm. In addition, states and regulatory agencies are more consistently fining companies for privacy violations.

The newest aspect of liability exposure within cyber policies are lawsuits alleging violation of data privacy laws that are not connected to data breaches or ransomware attacks. Often times, these claims are filed for violations of laws in connection with the collection and use of sensitive data. For instance, recent litigation in this area has focused on the use of technology that tracks user movement on a website or the use of biometric data to track employees and the hours they are working. The most challenging part about these claims is that only some cyber policies cover non-breach violations of data privacy laws, underscoring the need for a knowledgeable cyber broker.

BOTTOM LINE

Companies that fully implement effective defenses experience fewer and less severe claims as this makes it difficult for bad actors to gain access and limits the amount of information exposed in the event of a breach. Most insurers require certain protections before they will even consider insuring a given risk. Brokers with deep experience in cyber coverage can provide guidance on the kinds of defenses required by insurers. And beyond technical control requirements, the best cyber brokers can offer their clients risk modeling, evaluation of limit adequacy, external vulnerability scans and technology that provides a road map for IT security spending to help clients become best-in-class risks. AI-based security tools are also available to help companies quantify the number of records stored on their networks, and to identify older files that can be moved offline, which can be a challenging part of the risk management process.

Cyber coverage can be complex, with significant differences between carriers' terms and conditions. Given the potential costs of a cyber claim, it is important to seek policies offering full limits rather than sublimits and to avoid co-insurance. A knowledgeable cyber broker helps their clients decipher policy language differences and obtain robust coverage that will provide a key part of the organization's overall cyber defense strategy. Reach out to your CRC or INSUREtrust contact today for assistance.

CONTRIBUTORS

- Hunter Maskill is INSUREtrust's Managing Director where he co-manages the broking team, drives innovation by creating insurance products, and manages the firm's claims capabilities

- Chris Zepeda is an Associate Broker with CRC Group's Boca Raton, FL office and a member of the ExecPro Practice Group.

END NOTES

1. Ransomware groups don't die, they multiply, Corvus Insurance, April 30, 2024. https://info.corvusinsurance.com/hubfs/ransomware%20reports/RW%2024-1%20Q1%20Ransomware%20Report.pdf?
2. Ticketmaster hack may affect more than 500 million customers, NPR, June 1, 2024. https://www.npr.org/2024/06/01/nx-s1-4988602/ticketmaster-cyber-attack-million-customers
3. Form 8-K, Live Nation Entertainment Inc., May 31, 2024. https://www.sec.gov/Archives/edgar/data/1335258/000133525824000081/lyv-20240520.htm
4. UnitedHealth Group reports second quarter 2024 results, July 16, UnitedHealth Group, https://www.unitedhealthgroup.com/content/dam/UHG/PDF/investors/2024/UNH-Q2-2024-Release.pdf
5. UnitedHealth data breach caused by lack of multifactor authentication, CEO says, May 1, 2024, CBS News, https://www.cbsnews.com/news/unitedhealth-senate-hearing-cyberattack-change-healthcare/
6. UnitedHealth Group reports first quarter 2024 results, April 16, 2024, UnitedHealth. https://www.unitedhealthgroup.com/content/dam/UHG/PDF/investors/2024/UNH-Q1-2024-Release.pdf
7. CDK cyberattack expected to cost car dealers more than $1 billion, Michigan study says, Detroit Free Press, July 15, 2024. https://www.freep.com/story/money/cars/2024/07/15/cdk-cyberattack-cost-car-dealerships/74408247007/
8. How did the auto dealer outage end? CDK almost certainly paid a $25 million ransom, CNN, July 11. https://www.cnn.com/2024/07/11/business/cdk-hack-ransom-tweny-five-million-dollars/index.html
9. IBM Report; Half of breached organizations unwilling to increase security spend despite soaring breach coasts, July 24, 2023, IBM. https://newsroom.ibm.com/2023-07-24-IBM-Report-Half-of-Breached-Organizations-Unwilling-to-Increase-Security-Spend-Despite-Soaring-Breach-Costs
10. Monetization rates fall to record low despite jump in average ransom payments, July 21, 2023, Coveware, https://www.coveware.com/blog/2023/7/21/ransom-monetization-rates-fall-to-record-low-despite-jump-in-average-ransom-payments
11. SEC is investigating MOVEit mass-hack, says Progress Software, Oct. 11, 2023, TechCrunch.com, https://techcrunch.com/2023/10/11/sec-is-investigating-moveit-mass-hack-says-progress-software/
12. New ransomware reporting requirement kick in as victims increasingly avoid paying, Jan,. 26, 2024, Coveware. https://www.coveware.com/blog/2024/1/25/new-ransomware-reporting-requirements-kick-in-as-victims-increasingly-avoid-paying
13. U.S. & U.K. disrupt LockBit ranswomware variant, Feb. 20, 2024, U.S. Department of Justice, https://www.justice.gov/opa/pr/us-and-uk-disrupt-lockbit-ransomware-variant
14. Justice Department disrupts prolific ALPHV/Blackcat ransomware variant, Dec. 19, 2023, U.S. Department of Justice, https://www.justice.gov/opa/pr/justice-department-disrupts-prolific-alphvblackcat-ransomware-variant
15. What we know about the ransomware attack on a critical U.S. pipeline, NPR, May 10, 2021. See - https://www.npr.org/2021/05/10/995405459/what-we-know-about-the-ransomware-attack-on-a-critical-u-s-pipeline
16. Capital One Data Breach Class Action Settlement, Legal Notice, https://www.capitalonesettlement.com/Content/Documents/Notice.pdf