# Cyber Insurers:
## Vital Partners in the Battle Against Ransomware

Date: April 2020 | Authors: James Jaeger & Lawrence Wescott

*The explosion in ransomware over the past year has had a significant impact on businesses. Cyber insurers have been key players not only in helping their clients recover from ransomware attacks, but in taking proactive measures against them.*

### The Rise of Ransomware

Ransomware attacks increased substantially in 2019 in both size and impact. Attackers demonstrated a greater willingness to go after businesses, as opposed to consumers:

- In the Verizon 2019 Data Breach Investigations Report, ransomware was the second leading type of malware found by Verizon in the category "Top malware action varieties in incidents."[1]
- Arete tracked 33 different variant types in 2019, while seeing an increase of 56% of new variants tracked throughout the year.
- In an August 2019 report, security firm Malwarebytes found that ransomware attacks on business increased 365% between Q2 2018 and Q2 2019, while consumer detections declined.[2]
- The FBI's Internet Crime Complaint Center stated that "since early 2018, the incidence of broad, indiscriminate ransomware campaigns has sharply declined, but the losses from ransomware attacks have increased significantly, according to complaints received by IC3 and FBI case information....Ransomware attacks are becoming more targeted, sophisticated and costly, even as the overall frequency of attacks remains consistent."[3]

Malwarebytes Labs director Adam Kujawa explained that "what happened with WannaCry and NotPetya[4] revealed the underbelly of enterprise security." Before that, many people might have assumed that these are big companies, with security teams and it's hard for hackers to break in, but seeing how massive and damaging those attacks were — and not because of misconfigurations, but because of not patching in time — might have convinced more cybercriminals that it's worth going after businesses instead of consumers, he said.[5]

Some have accused cyber insurers of profiting from ransomware—that insurance serves as an incentive for such attacks. Marsh Senior Vice President and Assistant General Counsel for Cyber Policy Matthew McCabe characterizes this as "misinformation."[6] He observes that "under even modest scrutiny, this argument does not hold up. The truth is that ransomware attacks against businesses occur for one reason only: Criminals are succeeding."[7]

One reason for their success cited by McCabe is that many enterprises are failing to take necessary security precautions. According to Trend Micro CTO Raimund Genes, companies moved away from multiple offline backups in several places, and failed to implement basic security steps like network segmentation, as well as not implementing a comprehensive risk management plan.[8] In addition to

1 Verizon, 2019 Data Breach Investigations Report, pp. 11, 25, downloadable at https://enterprise.verizon.com/resources/reports/dbir/
2 Lucian Constantin, "More targeted, sophisticated and costly: Why ransomware might be your biggest threat," CSO United States, February 20, 2020, https://www.csoonline.com/article/3518864/more-targeted-sophisticated-and-costly-why-ransomware-might-be-your-biggest-threat.html
3 Id.
4 Ransomware variants which exploited vulnerabilities in the Windows Server Message Block protocol. The cost impact of WannaCry was estimated at $4 billion, while the cost of NetPetya was estimated at $1.2 billion. Dan Swinhoe, "Is the world ready for the next big ransomware attack?", CSO United States, March 4, 2019, https://www.csoonline.com/article/3345967/is-the-world-ready-for-the-next-big-ransomware-attack.html
5 Constantin, supra note 2.
6 Matthew McCabe, "Cyber Insurance Is Supporting the Fight Against Ransomware," Brink News, Oct 7, 2019, https://www.brinknews.com/cyber-insurance-is-supporting-the-fight-against-ransomware/
7 Id.
8 Varun Haran, "Why is Ransomware So Successful?", Bank Info Security, September 20, 2016, https://www.bankinfosecurity.com/interviews/interview-raimund-genes-ransom-

failed backups, backup solutions provider Veeam cites inadequate application of software patches, a failure to police user privileges in applications, which lead to more access than necessary, failure to implement multiple defenses against ransomware, and lack of user awareness against ransomware phishing scams.[9]

Another reason, according to McCabe, is that ransomware attacks are "cheap and easy to execute."[10] Threat actors are able to purchase ransomware at a low cost, or even for free on some forums, which makes the emergence of new strains of ransomware nearly a daily occurrence, stated IBM X-Force threat researcher Megan Roddie.[11] The widespread availability of ransomware tools led to the coining of the term "ransomware-as-a-service," based upon IT industry wide terms such as "software-as-a-service" or "platform-as-a-service."[12] These tools allow virtually anyone to launch a ransomware attack, even if they have little technical skills.[13]

## Cost Pressures

These factors, which, as previously noted, have resulted in a surge of ransomware attacks, have also taken their toll on insurers. Due to the frequency and breadth of these attacks, Reuters reported that some premiums had increased as much as 25%.[14] One reason is the cost of fulfilling claims. In many cases, once the victim's files are encrypted by the attacker, the victim has only two alternatives; either restore the files from a backup, assuming that the backup is good, or pay the ransom.[15]

A victim, particularly a small business, may be tempted by the number of free anti-ransomware tools on the Web, to try to remediate the effects of ransomware on their own, in order to mitigate these costs. However, this approach has a number of pitfalls. According to Arete Incident Response Principal Subject Matter Expert Harlan Carvey, one is that the use of such tools by those unfamiliar with them can end up causing additional damage and data corruption, obviating the ability for more knowledgeable agents to more fully recover data at some point in the future. Another is that improper use of the tools could result in the loss of important forensic evidence which could help trace the attacker.

One issue which a victim must address is whether the firm is obligated to notify its customers of a data breach under data breach notification laws. If the victim is a healthcare organization covered by the Health Insurance Portability and Accountability Act (HIPAA), the answer is presumed to be yes. The U.S. Department of Health and Human Services has taken the position that the presence of ransomware on the computers of a covered entity or business associate is a "security incident" under HIPAA.[16] Accordingly, under applicable regulations, a breach under HIPAA is presumed to have occurred, thus triggering the breach notification provisions in 45 CFR Subpart D, unless the victim can demonstrate that there was a "low probability" that the protected health information (PHI) has been compromised based on four factors, including whether the PHI was actually acquired or viewed.[17] The burden of proof is on the victim to establish that the use or disclosure did not constitute a breach.[18] Thus, if the victim is covered under HIPAA, and believes that PHI was not encrypted, the victim would need to engage forensic analysis services to provide the needed proof that PHI was not encrypted. These types of costs are generally covered under cyber insurance policies.

Under state data breach notification laws, the obligation to notify firm customers of a ransomware event depends upon the language of a given state's law. For example, in Colorado, a "security breach" triggering a notification obligation is "the unauthorized acquisition of unencrypted computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a covered entity."[19] For ransomware that only encrypts a victim's data, the attacker might not have "acquired" the data. Nevertheless, the determination of whether notification is required is a very fact-specific one which requires the advice of an

ware-virus-total-issue-i-3328
9 Nick Cavalancia, "Why is Ransomware Still So Successful?", Veeam Blog, January 20, 2018, https://www.veeam.com/blog/reasons-for-successful-ransomware-attack.html.
10 McCabe, supra note 6
11 Lindsey O'Donnell, "Researchers Warn of Novel PXJ Ransomware Strain," Threatpost, March 12, 2020, https://threatpost.com/novel-pxj-ransomware-strain/153673/
12 See, e.g. Vladamir Unterfingher, "Ransomware as a Service (RaaS) – A Contemporary Mal du siècle?", Heimdal Security, November 11, 2019, https://heimdalsecurity.com/blog/ransomware-as-a-service/.
13 Jalal Bouhdada, "Ransomware: A Serious OT Security Threat", Applied Risk, March 4, 2020, https://applied-risk.com/resources/ransomware-a-serious-ot-security-threat.
14 Scott Ikeda, "Ransomware Attacks Are causing Cyber Insurance Rates to Go Through the Roof; Premiums up as Much as 25 Percent", CPO Magazine, February 10, 2020, https://www.cpomagazine.com/cyber-security/ransomware-attacks-are-causing-cyber-insurance-rates-to-go-through-the-roof-premiums-up-as-much-as-25-percent/
15 Id.
16 U.S. Dept. of Health and Human Services, "FACT SHEET: Ransomware and HIPAA", located at https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf.
17 45 C.F.R. § 164.402(2).
18 45 C.F.R. § 164.414(b).
19 Colo. Rev. Stat. Ann. § 6-1-716(h) (LexisNexis 2020).

attorney versed in the state's laws. However, in Florida, a breach of security triggering a notification obligation is defined as "unauthorized access of data in electronic form containing personal information."[20] There is no question that an attacker who has encrypted covered information has "accessed" it.

Late in 2019, the Maze ransomware variant coupled the encryption of the victim's data with a threat to publish the data on a website. The attackers exfiltrated the data prior to encrypting it – thus, triggering a notification requirement under any scenario. Arete Incident Response Director Evgueni Erchov has observed that this technique has been copied by other attackers (REvil/Sodinokibi, DopplePaymer, Mespinoza and AKO). One commentator has stated that all ransomware attacks should now be considered data breaches.[21]

Erchov notes that the following activities are recommended for firms experiencing a ransomware event:

- Initial triage and containment efforts to ensure that the attackers no longer have access to systems and networks.
- Legal assessment to identify all applicable obligations under state and federal laws and regulations (such as the above notification issue).
- Forensic evidence collection and preservation.
- Recovery of data and systems (this can occur either by paying the ransom, restoring from backups, or rebuilding systems and data from scratch).
- Digital forensics investigation.

If the results of the forensics investigation do not rule out data access or exfiltration, he recommends these additional activities:

- Collection and data mining of compromised data to identify all personally identifiable information/payment card information/protected health information records.
- Legal review of results.
- Notifications of individuals and organizations whose data was compromised.
- DarkWeb search and monitoring services to proactively detect if compromised data would get posted on hacker forums or underground markets.[22]

Other characteristics of the cyber insurance market in general contribute to cost pressures:

- Current threats adapt and evolve while all-new hacks present themselves without warning.
- Cyber is a relatively young product line lacking the data and actuarial methodology to model risk as compared to much more established and more static insurance products such as auto and homeowners.
- Since the potential damage and scope of a cyber event are relatively unknown, accumulation presents greater potential exposure especially as market share grows.[23]

All of these forces have contributed to an asymmetric perfect storm. The victim incurs significant costs in order to recover from an attack (covered by cyber insurance), while the attackers' costs may be minimal. Cyber insurers thus have strong incentives to reduce costs by taking proactive measures to help their insureds more effectively defend against ransomware attacks.

## Cyber Insurers - Allies in the Battle Against Ransomware

Most carriers are working with their insureds to take more effective measures against ransomware. Some efforts include a greater willingness to underwrite firms that have added network features to prevent attacks from spreading through systems, while others may require policyholders to have data-backup procedures.[24] Scott Ikeda, senior correspondent at CPO Magazine, noted that "cyber insurance rates now often take into account an organization's IT security and preparedness for cyber risks. Measures specific to ransomware mitigation, such as regular backups and a tested incident response plan, can help."[25]

20 Fla. Stat. Ann. §501.171(1)(a) (LexisNexis 2020).
21 Lawrence Abrams, "Three More Ransomware Families Create Sites to Leak Stolen Data," Bleeping Computer, March 24, 2020, https://www.bleepingcomputer.com/news/security/three-more-ransomware-families-create-sites-to-leak-stolen-data/.
22 Arete Incident Response Crimeware Report, April, 2020, www.areteir.com.
23 Asaf Lifshitz, "Cyber insurance challenges: Meeting your business needs," NU Property Casualty 360, February 27, 2020, https://www.propertycasualty360.com/2020/02/27/cyber-insurance-challenges-meeting-your-business-needs.
24 Suzanne Barlyn, "Ransomware Exposure Driving Up Cyber Insurance Costs,", Insurance Journal, Jan. 22, 2020, https://www.insurancejournal.com/news/national/2020/01/22/555479.htm
25 Ikeda, supra note 14.

Another commentator argues that cyber insurers "can reshape cybersecurity." Insurers have the same goal as the insured-not to get breached. Insurers collect proprietary information about their insureds not available to other companies. They have the ability to identify the type and severity of breaches and associate them with actual losses. Carriers can analyze this information to determine the root causes of attacks and how to minimize future ones. They can analyze the results of the technical solutions used by their clients and assess their overall effectiveness. Carriers can also require an applicant to provide additional quantitative and qualitative data in order to better understand overall risk level faced by the insured. He concludes: "Once insurance carriers can understand and model cyber risk, they can drive adoption of best practices via financial incentives to the insureds."[26]

Carriers often emphasize preventive measures that can be taken in their own publications. Beazley's 2020 Breach Briefing focuses on ransomware—containing information and statistics on the types of ransomware incidents handled by Beazley Breach Response Services, case studies, and tips on how to prevent infection by ransomware.[27] AIG offers advice on protecting open source databases from ransomware attacks.[28] Chubb provides proprietary advice to its policyholders on how to detect and prevent ransomware,[29] while providing reports to the public on ransomware variants and best practices on prevention.[30] Travelers has posted a video and infographic on the current ransomware landscape along with information regarding prevention.[31] A white paper on cyber resilience is also available from Travelers.[32]

Matthew McCabe observes that the cyber insurance underwriting process "raises awareness of threats, identifies how companies should be responding, and educates insureds." He adds that after an attack, insurers convene "the right team of experts, including legal counsel and forensic experts, to assess the incident and recommend appropriate action in a timely fashion." He concludes: "Companies are fighting hackers on an unbalanced playing field, where defense is much harder than offense, and cyber insurance has proven to be a valuable partner in that fight. Given the stakes, companies should be eager to take all the help they can get."[33]

## Conclusion

Ransomware trends indicate that attacks will only increase in size and severity. As cost pressures increase, cyber insurers will accordingly incent their insureds to adopt more effective defensive measures. Accordingly, cyber insurers play a valuable role not only in helping their insureds recover from an attack, but by helping their insureds take steps to decrease the likelihood of attacks.

## About the Authors


**James Jaeger**

James Jaeger, president and chief cyber strategist, Arete Incident Response, is a 25-year cybersecurity industry veteran, who's always been eyes on the network and at the forefront of national security issues. He's held leadership roles in industry as well as at the National Security Agency and Air Force and has often been called in to brief intelligence directors at various federal agencies including the Department of Defense and CIA. He brings a passion for robust, continuous network monitoring to his decades of expertise fighting cyber crime. His cyber expertise includes leading complex forensic investigations, network incident response operations, network security monitoring and engineering and working with customers and authorities to assist in the pursuit and prosecution of cyber criminals.

**Lawrence Wescott**

Larry is a cybersecurity strategist at Arete Incident Response. He develops continuing legal education programs on cybersecurity for Arete's law firm and insurance partners.He is a former system administrator, IT manager, database application development manager, and IT consultant. He is a contributor to two Sedona publications: The Sedona Conference Primer on Social Media (first edition), and The Sedona Conference Commentary on Rule 34 and Rule 45 "Possession, Custody, or Control," and has published multiple articles on data privacy and retention. Larry received his law degree with honors from the University of Maryland and holds a masters in business administration from the University of Georgia. He is also a Certified Information Systems Security Professional (CISSP).


26 Asaf Lifshitz, "Cyber Insurance Will Reshape Cybersecurity," Insurance Journal, October 11, 2019, https://www.insurancejournal.com/news/national/2019/10/11/545228.htm.
27 Beazley Breach Briefing 2020, March 23, 2020, downloaded from https://www.beazley.com/news/2020/beazley_breach_briefing_2020.html
28 AIG Alert, "Open Source Databases Are a Target for Recent Ransomware Attacks," https://www.aig.com/content/dam/aig/america-canada/us/documents/business/cyber/cyber-mongodb-alert-012617-final.pdf
29 See https://www.chubb.com/us-en/cyber-risk-management/.
30 Chubb Cyber InFocus, October, 2019, https://www.chubb.com/us-en/_assets/doc/cyber-infocus_10.10.19.pdf.
31 Travelers, "What is the Current Ransomware Landscape?", https://www.travelers.com/business-insights/topics/cyber/what-is-the-current-ransomware-landscape
32 Travelers and Symantec, "Building Resilience to Cyber Risk," https://www.travelers.com/iw-documents/cyber-insurance/cyber-risk-whitepaper.pdf.
33 McCabe, supra note 6