ESG BRIEF

Ransomware Still Rampant, Fueled by Insurance Companies

Date: February 2020 **Author:** Dave Gruber, Senior Analyst, and Bill Lundell, Director of Syndicated Research

ABSTRACT: While ransomware is not a new cyber-threat, largely entering the cybersecurity scene in 2016 and 2017 with a number of high-profile attacks, research conducted by ESG reveals that a majority of organizations continued to experience ransomware attacks in 2019, representing a concern for both business and IT leadership teams. The research further reveals the prominence of cybersecurity insurance policies, and the relationship between ransomware payouts and those companies that hold these policies. A subset of organizations with cybersecurity insurance report that their providers are advising, and possibly even pressuring, them to pay cyber ransoms, further fueling the success rates and the economy built around ransomware. This disturbing trend sets the stage for the continuance of ransomware, and an opportunity for criminals to exploit those organizations that have engaged with cybersecurity insurance companies.

Overview

ESG recently completed its annual technology spending intentions survey of 658 senior IT decision makers at midmarket (i.e., 100 to 999 employees) and enterprise (i.e., 1,000 or more employees) organizations across North America and Western Europe.[1] As part of that research, respondents were asked about their organization's experience with ransomware over the past 12 months. While a significant number of endpoint security and data protection solutions expound upon their ability to recognize and prevent ransomware, the threat landscape for net-new ransomware strains continues to grow, with bad actors attempting to prey on vulnerable organizations that either can't afford these solutions, or lack controls to ensure the vulnerabilities often exploited by ransomware are patched. According to Figure 1, nearly two-thirds (60%) of organizations experienced a ransomware attack in 2019, with 29% reporting that attacks happened on a weekly basis (or even more frequently).

From an industry perspective, the majority of organizations—regardless of vertical—experienced at least one attempted ransomware attack over the past 12 months (see Table 1). Technology and healthcare were not only the two likeliest sectors to have been subjected to ransomware in 2019, but they were also significantly more likely than their counterparts in all other industries to have been targeted on a daily or weekly basis. Healthcare organizations tend to operate a wide variety of connected devices, many of which often fall behind in the software patching required to close known vulnerabilities, making them attractive targets for criminals. With patient care at risk and lots of complexity in restoring data from backups, they are more likely to give in and pay ransoms. Technology companies, while a less obvious target, have significant digital intellectual property, which entices bad actors.

[1] Source: ESG Master Survey Results, *2020 Technology Spending Intentions Survey*, January 2020.

Figure 1. Rate of Ransomware Attacks over the Course of 2019

Source: Enterprise Strategy Group

Table 1. Rate of Ransomware Attacks over the Course of 2019, by Industry

To the best of your knowledge, has your organization experienced an attempted ransomware attack within the last 12 months?	Technology (N=127)	Healthcare (N=53)	All other industries (N=564)
Yes, on a daily basis	26%	15%	7%
Yes, on a weekly basis	29%	21%	13%
Yes, on a monthly basis	13%	21%	12%
Yes, on a sporadic (i.e., less than monthly) basis	16%	19%	28%
No, we have not experienced any attempted ransomware attacks	16%	25%	35%

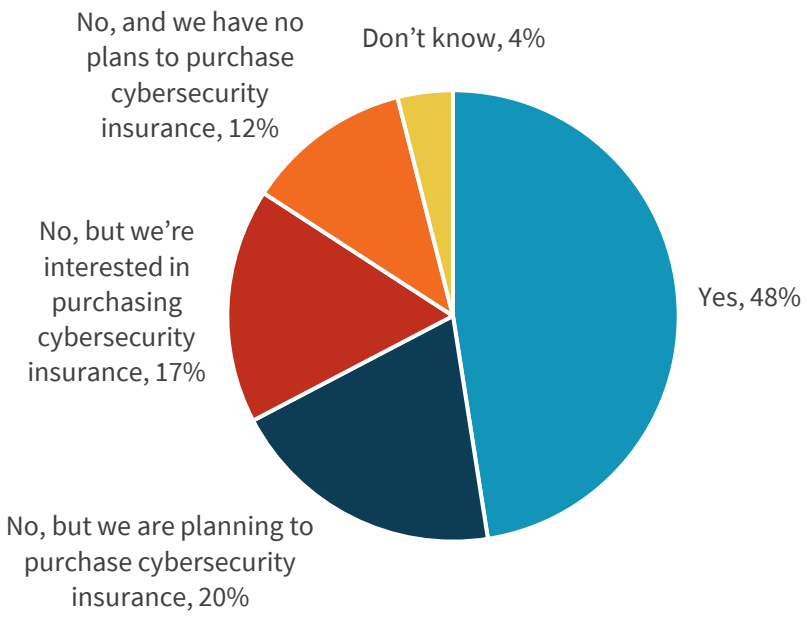
Source: Enterprise Strategy Group

Cybersecurity insurance is designed to mitigate losses from a variety of cyber incidents, including data breaches, business interruption, and network damage. Nearly half (48%) of organizations have purchased cybersecurity insurance while another 37% have either plans for or interest in doing so (see Figure 2). As CFOs assess the remediation costs together with the brand and IP risk associated with ransomware and other cyber-attacks, buying insurance makes good financial sense.

While certainly not the only driver of cybersecurity insurance purchases, it is not surprising to see a connection to an organization's 2019 ransomware experience. Specifically, Figure 3 reveals that 85% of the organizations that experienced ransomware attacks on a daily basis over the last year currently have cybersecurity insurance—compared with only 38% of organizations that did not experience any ransomware attacks over the same period. This connection demonstrates the risk mitigation practices that are becoming commonplace today.

Figure 2. Cybersecurity Insurance Is Gaining Market Traction

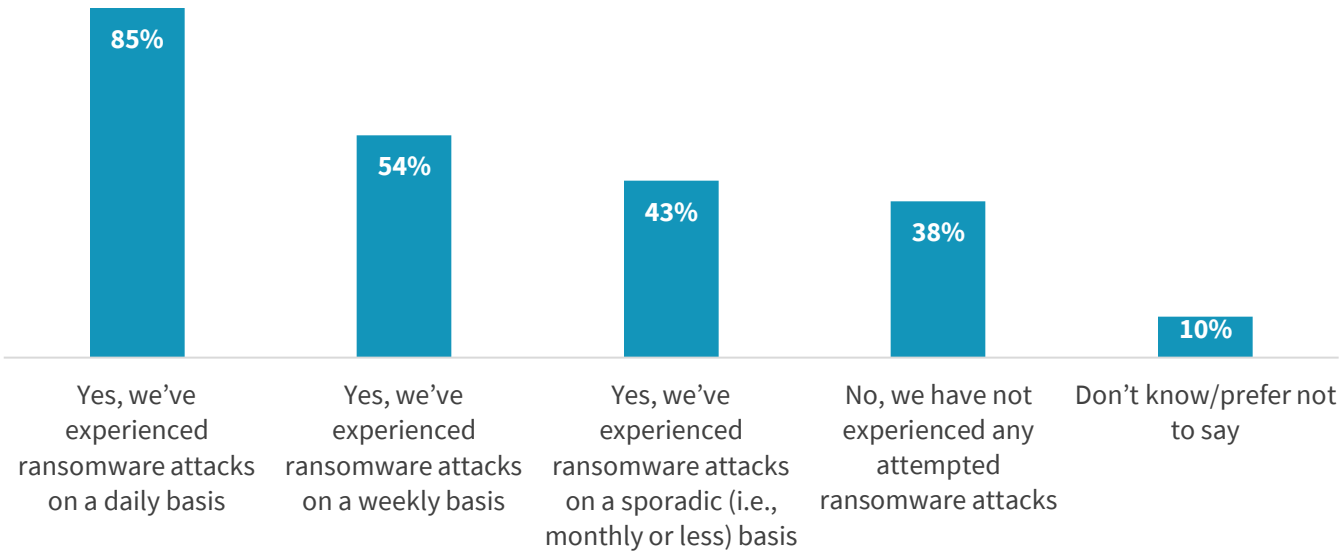
Does your organization have cybersecurity insurance? (Percent of respondents, N=658)



Source: Enterprise Strategy Group

Figure 3. Cybersecurity Insurance Much More Prevalent among Frequent Ransomware Targets

Percentage of organizations that currently have cybersecurity insurance based on frequency of ransomware attacks over last 12 months. (Percent of respondents)



Source: Enterprise Strategy Group

How does the connection between ransomware attack frequency and cybersecurity insurance vary based on industry vertical? According to Table 2, for the majority of sectors, there is a significant gap between the percentage of organizations

that have experienced an attempted ransomware attack within the past year and the percentage that currently have a cybersecurity insurance policy. In fact, financial services is the *only* industry with more organizations in possession of a cybersecurity insurance policy than those organizations that have experienced an attempted ransomware attack. At the other end of the spectrum, technology, education, and government are the verticals with the biggest ransomware/cybersecurity insurance gaps. With state and local governments hit so hard over the past year, they would seem like obvious candidates for cybersecurity insurance; however, most lack the budgets to purchase it. K-12 education faces the same issue. With the intense, public media coverage of these attacks, most will likely have better luck securing funding in their next budget cycles.

Table 2. Industries with the Biggest Ransomware/Cybersecurity Insurance 'Gaps'

Industry perspective on frequency of ransomware attacks and ownership of cybersecurity insurance:			
	Percentage of organizations that experienced a ransomware attack	Percentage of organizations with cybersecurity insurance	Ransomware attack/cybersecurity insurance "gap"
Technology	84%	60%	-24%
Healthcare	75%	62%	-13%
Education	68%	38%	-30%
Communications & media	64%	60%	-4%
Manufacturing	54%	41%	-13%
Retail/wholesale	49%	55%	+6%
Government	48%	32%	-16%
Business services	47%	35%	-12%
Financial	43%	40%	-3%

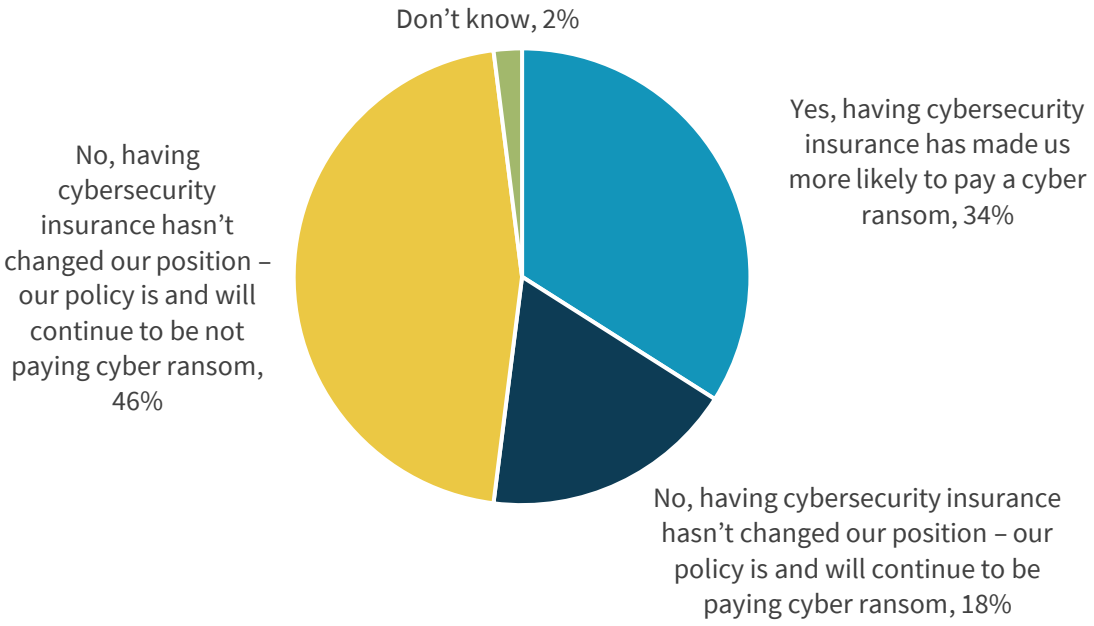
Source: Enterprise Strategy Group

Among those organizations that currently have cybersecurity insurance, more than one-third (34%) say that having cybersecurity insurance has made them more likely to pay a cyber ransom, while 64% claim that having cybersecurity insurance has not changed their position in either direction (see Figure 4). It is worth noting that more than half (52%) of these organizations claim their current policy is to pay cyber ransoms.

Are cybersecurity insurance providers attempting to exert their influence in ransomware situations? It would appear so as 84% of organizations that say that having cybersecurity insurance has made them more likely to pay a cyber ransom report being advised or pressured by their provider to do so (see Figure 5). It's not a coincidence that ransomware attacks have been on the rise in the past year. With payouts happening with regularity, criminals are paying attention to the kinds of organizations that are most willing to pay. Public industry data further informs criminals about those industries that are engaging with cybersecurity insurance companies. This all supports the larger criminal economy growth rate associated with ransomware.

Figure 4. Cybersecurity Insurance Is Having an Impact on Ransomware Payment Strategies

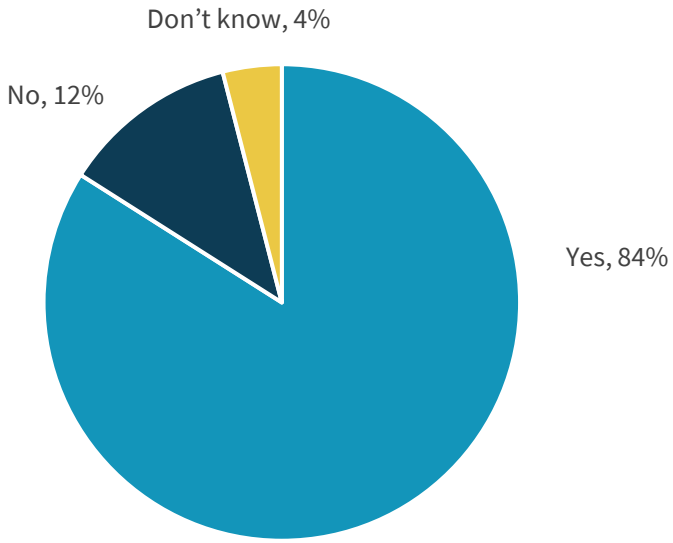
Has having cybersecurity insurance changed your organization's position on paying cyber ransom? (Percent of respondents, N=314)



Source: Enterprise Strategy Group

Figure 5. Cybersecurity Insurers Are Exerting Their Influence in Ransomware Situations

Has your organization's cybersecurity insurance provider advised or pressured you to pay a cyber ransom? (Percent of respondents, N=108)



Source: Enterprise Strategy Group

The Bigger Truth

With the continuance of ransomware attacks across all industries, organizations need to protect themselves from the associated financial and operational risks. With cybersecurity insurance playing a key role in risk mitigation strategies, and with insurance companies recommending that organizations pay off criminal ransomware demands, the ransomware threat is likely to continue to grow rapidly, fueled by the simple financial tradeoff delivered on a silver platter by cybersecurity insurance providers. Ransoms will continue to rise as criminals see a trend in successful payouts. This is a no-win situation.

Criminals are closely watching the financial tolerances of both companies and insurance providers, carefully orchestrating their demands to increase the likelihood of payouts. This cat-and-mouse game has created a multibillion dollar, illegal economy fueled by both the inability to keep ransomware out, and the willingness of cybersecurity insurance companies to manage costs by paying off criminals.

Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides market intelligence and actionable insight to the global IT community.

www.esg-global.com contact@esg-global.com 508.482.0188