

*Ransomware Amidst a Pandemic:  
Potential for Catastrophic Loss If  
Stringent Cybersecurity Protocols Are  
Not Followed*

*Akhil Chopra and Elissa Doroff*



# Ransomware Amidst a Pandemic

*Potential for Catastrophic  
Loss If Stringent Cybersecurity  
Protocols Are Not Followed*



Ransomware demands and payments continue to escalate. In fact, cyber risk assessment firm NetDiligence found the average requested ransom amounts rose 200% from 2018 to 2019, averaging \$115,123 in 2019.<sup>1</sup> According to Crypsis Group, a leading digital forensics company, the highest ransom paid was on average \$5 million and the highest demand was \$15 million.<sup>2</sup>

## WHAT IS RANSOMWARE?

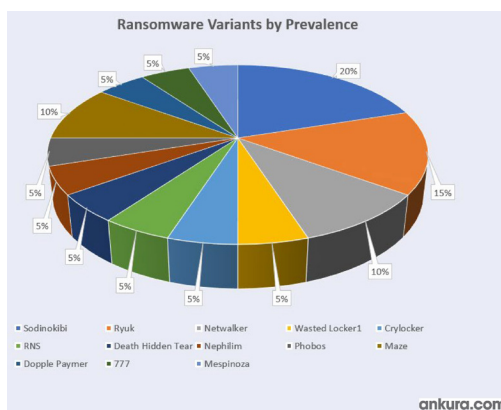
Simply stated, ransomware is a type of malware designed to deny access to a computing system or data (usually via encryption) until a ransom is paid.<sup>3</sup> In 2012 when ransomware first emerged on the cyber landscape, demands were anywhere from \$500 to \$50,000. With demands today in excess of \$20 million, it has become clear these numbers are not going down. Ransomware has become an increasingly prevalent threat to organizations worldwide and recent attacks have shown that all companies, regardless of industry or size, are at risk.

Ransomware is an ever-evolving attack tool and even the simplest form can cost a company significant time and money. The more severe strains can cripple a company completely. Even worse, hackers have a tendency to duplicate successful attacks and hit victims repeatedly. In addition to the actual ransom payment, companies suffering downtime, even if not significant, are likely to experience a substantial decrease in consumer trust. According to Coveware, the average number of days companies were down due to an attack is 16.<sup>4</sup>

While all industries may fall prey to an attack, governments, educational institutions and professional services firms are frequent targets due to their lack of cybersecurity preparedness, typically resulting from a lower budget compared with larger, more regulated industries.

The most common ransomware attack vectors are remote desktop protocol compromise, email phishing and software vulnerabilities.<sup>5</sup>

## RANSOMWARE VARIANTS



While there are several ransomware variants, the more popular ones intend to steal data, and include MAZE, Nemty, Sodinokibi, Ryuk, Netwalker, Nephilim, Defray 777 and Wasted. Hackers deploy various techniques in attempting to extort their victims; most commonly, they leak samples of their victim's data on the internet or dark web. If their victim does not comply, they leak everything they took. Victims then have to deal with both a ransomware attack and a data breach at the same time — turning a costly situation into a catastrophic event.

The costs associated with these varying strains of ransom vary greatly. According to the global cybersecurity firm Ankura, based on the matters they have managed, the average ransom payments associated with Sodinokibi and Ryuk were approximately \$400,000, Crylocker was approximately \$620,000 and others fell anywhere in between.<sup>6</sup>

Some costs cannot be monetized even if a company needs to pay to decrypt their data. Specifically, any company who fell prey to the Wasted variant and wants to pay the ransom can no longer do so due to a recent decision by the Office of Foreign Assets Control (OFAC).

This was due to the fact that payment of the ransom would be associated too closely with Evil Corp which would violate OFAC's Economic Sanctions Enforcement Guidelines. As a consequence of OFAC's decision, there are limited options — none of which are ideal:



1. Pay it yourself (and risk being in violation of the law).
2. Find another middleman (it's unlikely anyone else wants to take the risk).
3. Apply for a license and hope OFAC treats you differently (this is unlikely, and even if they do your threat actor would probably be long gone by the time you get a decision).

## SIMPLE BEST PRACTICES

While ransomware attacks are prevalent and increasing in cost, there are several basic risk mitigation techniques companies can employ to avoid falling prey to an incident. They include:

- **Educate and regularly test employees.** Conduct regular social engineering and phishing campaigns so employees can recognize suspicious emails and avoid clicking on unfamiliar links.
- **Back up your files often,** ideally on a cloud backup service.
- **Segment your networks** to keep critical computers isolated and prevent the spread of malware in case of attack.
- **Lock down admin rights** on desktops and disable remote desktop protocols (unless and until there is multi-factor authentication (MFA) in place).
- **Patch often** to avoid falling prey to known vulnerabilities that hackers target. Include desktops, laptops, servers, applications, browsers, mobile devices and web plugins. This includes turning off any auto-update features.
- **Have a crisis plan.** This includes having pre-established relationships with expert privacy counsel and cybersecurity vendors. Since ransomware payments are usually demanded in the form of cryptocurrency, it is important to ensure your cybersecurity vendor has a bitcoin wallet.

## THE ROLE OF INSURANCE

The aforementioned practices may seem onerous and costly for some organizations. Positively, there is another risk transfer solution to mitigate the potential costs — cyber liability insurance. Historically a throw on coverage known as “cyber-extortion,” the ransomware insuring agreement is the most important coverage on a cyber liability insurance policy. Ransomware coverage will provide the costs associated with a ransomware incident, such as hiring the appropriate legal and forensic vendor to investigate the attack to determine what information has been compromised, and ultimately, whether payment of the ransom should be made as well as the payment itself, subject to the insurance term, conditions and limits of liability. In addition, cyber insurance provides several proactive resources to assist companies in understanding their cybersecurity risks and the best practices outlined above to help prepare for a ransomware attack.

Given the increase in frequency and severity of ransomware demands and payments, cyber insurance carriers are now doing more due diligence in underwriting risks. Companies can expect some additional questions on applications around file backups, recovery time objectives, network accessibility, the use of multi-factor authentication, network segmentation and protocol around web and email filtering.

Undoubtedly, this upward trend in ransomware is directly impacting the cost of cyber insurance. What companies are likely to notice however, are gradually increasing premiums compared with what they might have obtained coverage for in prior years.

In conclusion, ransomware shows no signs of slowing down. In fact, just the opposite. With demands and payments increasing in both frequency and severity further complicated by the struggle to keep ahead of the hackers and varying strains, companies must employ moderate cybersecurity protocols to avoid being the next victim. Either through their own IT, partnering with third party cybersecurity firms, transferring the risk to Insurance, or ideally all of the above, actions are required to avoid being the next victim.

**For more information, please contact the NFP Cyber team with any questions:  
Akhil Chopra at [akhil.chopra@nfp.com](mailto:akhil.chopra@nfp.com) or Elissa Doroff at [elissa.doroff@nfp.com](mailto:elissa.doroff@nfp.com).**

### Sources:

- <sup>1</sup> 2020 Spotlight on Ransomware, NetDiligence, 2020; [https://netdiligence.com/wp-content/uploads/2020/02/NetD\\_2020Spot\\_Ransomware.pdf](https://netdiligence.com/wp-content/uploads/2020/02/NetD_2020Spot_Ransomware.pdf)
- <sup>2</sup> 2020 Incident Response and Data Breach Report, Crypsis Group, 2020; <https://register.crypsisgroup.com/cybersecurity-threat-report>.
- <sup>3</sup> 2020 Incident Response and Data Breach Report, p. 9, Crypsis Group, 2020; <https://register.crypsisgroup.com/cybersecurity-threat-report>.
- <sup>4</sup> “Costs of Ransomware Attacks in Q1 2020,” Ransomware Attacks Fracture Between Enterprise and Ransomware-as-a-Service in Q2 as Demands Increase, Coveware, 2020; <https://www.coveware.com/blog/q2-2020-ransomware-marketplace-report#types>
- <sup>5</sup> “Comparing the Top 3 Types of Ransomware - Sodinokibi, Maze and Phobos,” Ransomware Attacks Fracture Between Enterprise and Ransomware-as-a-Service in Q2 as Demands Increase, Coveware, 2020; <https://www.coveware.com/blog/q2-2020-ransomware-marketplace-report#types>
- <sup>6</sup> The Shifting Cybersecurity Landscape, Ankura and ARI Kaplan Advisors, 2018; <https://ankura.com/wp-content/uploads/2018/02/the-shifting-cybersecurity-landscape.pdf>

This information has been provided as an informational resource for NFP clients and business partners. It is intended to provide general guidance, and is not intended to address specific risk scenarios. Regarding insurance coverage questions, each specific policy must be reviewed in its entirety to determine the extent, if any, of coverage available for the impact of the Coronavirus. If you have questions, please reach out to your NFP contact. This document does not amend, extend, or alter coverage. Insurance services provided by NFP Property & Casualty Services, Inc. (NFP P&C), a subsidiary of NFP Corp. (NFP) and related NFP subsidiary companies. In California, NFP P&C does business as NFP Property & Casualty Insurance Services, Inc. License #0F15715. Neither NFP nor its subsidiaries provide tax or legal advice.