REVISED JANUARY 2023

# Ransomware
## CYBER RISK TOOLKIT

American Academy of Actuaries
Committee on Cyber Risk, Casualty Practice Council

American Academy of Actuaries
ACTUARY.ORG

**The American Academy of Actuaries' Cyber Risk Toolkit, developed by the Academy's Committee on Cyber Risk, is a series of papers addressing issues pertinent to cyber risk insurance and cyber exposure. This toolkit is intended to be a resource for interested readers of the general public, public policymakers, the actuarial profession, the insurance sector, and other stakeholders.**

**While the paper that follows stands alone, the complete toolkit offers a cohesive overview of the challenges posed in the cyber insurance market. The toolkit will be updated periodically to reflect new and emerging work from the committee.**



American Academy of Actuaries

AMERICAN ACADEMY OF ACTUARIES
1850 M STREET NW, SUITE 300, WASHINGTON, D.C. 20036
202-223-8196 | **ACTUARY.ORG**

# Ransomware

Revised January 2023

**Cybercrime is expected to keep growing as businesses increasingly rely on remote workers and the internet of things (IOT) continues to expand. One type of cybercrime that is rapidly increasing is ransomware attacks. According to insurance industry experts, ransomware became the biggest cyber threat facing businesses over 2019 and 2020.[1] Ransomware has many consequential effects from temporary or permanent loss of data and complete shutdown of operations, to rendering hardware inoperable. The victim is instructed to pay a ransom, generally in bitcoin, with a promise of reversing the malware damage (restoring access to systems or data, etc.).**

Some ransomware criminals are going beyond just the shutdown of operations and are also threatening to release the data on the dark web if the ransom is not paid. This is called double extortion ransomware. For triple extortion, the criminal may even contact and threaten customers whose data has been stolen.[2]

The earliest example of ransomware is PC Cyborg, which was spread by infected floppy disks in 1991.[3] Today there are many avenues through which ransomware might victimize potential targets—email, downloads, malicious online advertisements, cloud storage, and others.

Ransomware victims face choosing between paying the ransom or investing the cost and time in repairing the infected system. After a 2016 ransomware attack on San Francisco's Municipal Transportation Agency (SFMTA), the agency chose not to pay the ransom and relied on backup systems to restore affected computers. Ticket machines and faregates were turned off for three days in order not to inconvenience passengers.[4] The city of Atlanta during a ransomware attack in 2018 chose not to pay a ransom demand of $50,000 in bitcoin and spent more than $7 million on recovery costs as of June 2019.[5]

1 "Frequency of Cyber Events Targeting Businesses Increasing: Travelers"; MyNewMarkets powered by *Insurance Journal*; Dec. 11, 2020.
2 "Triple Threat: Ransomware Criminals Add Data Theft, Manipulation to Encryption Tactics"; *Insurance Journal;* March 30, 2022.
3 "Ransomware: Reinsurance Association of America"; 2021.
4 SFMTA Blog, Nov. 28, 2016.
5 "Don't Pay Cyber Ransoms, Officials Warn"; *WSJ Pro*; Feb. 12, 2020.

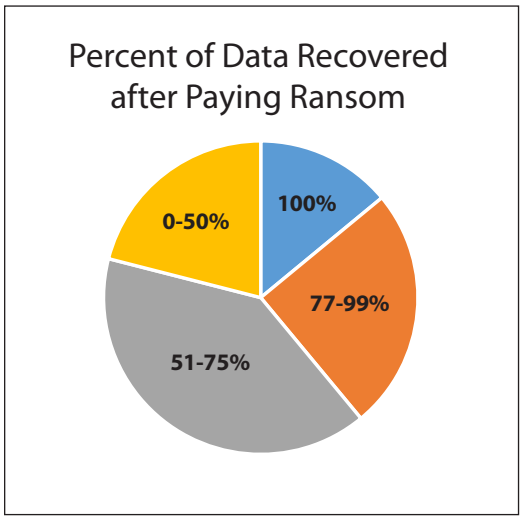
# To pay or not to pay?

As shown in the table below, some ransomware victims ended up paying considerably more than the ransom demand to restore their systems. There is also a trend of ransomware demands significantly increasing over time:

**Table 1**

| Entity | Year | Ransomware-Demand | Ransomware-Paid (Y/N) | Cost to Repair If N |
|---|---|---|---|---|
| Atlanta, Georgia | 2018 | $50,000 | N | $7,000,000 |
| Baltimore, Maryland | 2019 | 80,000 | N | 18,000,000 |
| Newark, New Jersey | 2018 | 30,000 | Y | |
| U.S. County infected by Ryuk | N/A | 132,000 | Y | |
| U.S. City infected by Robbinhood | N/A | 76,000 | N | 9,000,000 |
| U.S. County infected by Ryuk | N/A | 1,200,000 | N | 1,000,000 |
| Colonial Pipeline | 2021 | 4,400,000 | Y | |
| JBS Foods | 2021 | 11,000,000 | | |

In a survey of 620 information technology and cybersecurity professionals in North America and western Europe, 56% responded that they did pay the ransom to recover from a ransomware attack. Even among those paying the ransom, only a minority recovered all their data as shown below.[6]




6 "Organizations are Better Prepared to Fight Ransomware but Gaps Remain", Tech Republic, April 12, 2022.

There are several reasons advocated by the Federal Bureau of Investigation (FBI) not to pay the ransom demand:

- Emboldens adversaries to target additional organizations
- Encourages criminals to use ransomware to fund illicit activities
- Does not guarantee files will be recovered[7]

## Does paying ransom increase risk of getting another attack?

One concern with paying a ransom is that the targeted organization/entity will be marked as a receptive target for future ransomware attacks. However, while larger organizations may receive targeted attacks (such as "big game ransomware"), smaller organizations are more likely to be caught in a mass scanning approach wherein hackers cast a wide net for victims by exploiting a specific weakness in cyber systems. Hence, an organization's size may be a consideration in whether or not to pay a ransom.

Others disagree that the risk of getting attacked increases after paying ransom. According to international insurance brokerage and risk adviser company Marsh, victims are rarely "targeted"—instead, attackers select a specific vulnerability to exploit and use the vulnerability as a wide net to try and bring in as many victims as possible.[8] Similar comments were made during a webinar by Advisen.[9] On the other hand, the attack-and-penetration landscape changes continuously and in new directions and new ways.

## Where is the ransom money going?

In late 2020, the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) issued an advisory regarding the risk of sanctions associated with ransomware payments. If the victim chooses to pay the ransom and the ransomware payment goes to an individual or entity on OFAC's Specially Designated Nationals and Blocked Persons List, OFAC may impose civil penalties on the ransomware victim.[10] This is challenging as generally a criminal's identity and associations are not known. An updated advisory was issued in September 2021 and addressed mitigating factors that may impact OFAC's response, including the ransomware victim's cooperation with OFAC and law enforcement.[11]

7 "Ransomware, What It Is & What To Do About It"; National Cyber Investigative Joint Task Force.
8 "Cyber Insurance is Supporting the Fight Against Ransomware"; Marsh JLT Specialty; October 2019.
9 "Advisen Quarterly Cyber Risk Trends: 2020 Wrap-Up Webinar"; Feb. 3, 2020.
10 Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments; U.S. Department of the Treasury; Oct. 1, 2020.
11 Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments; U.S. Department of the Treasury; September 21, 2021.

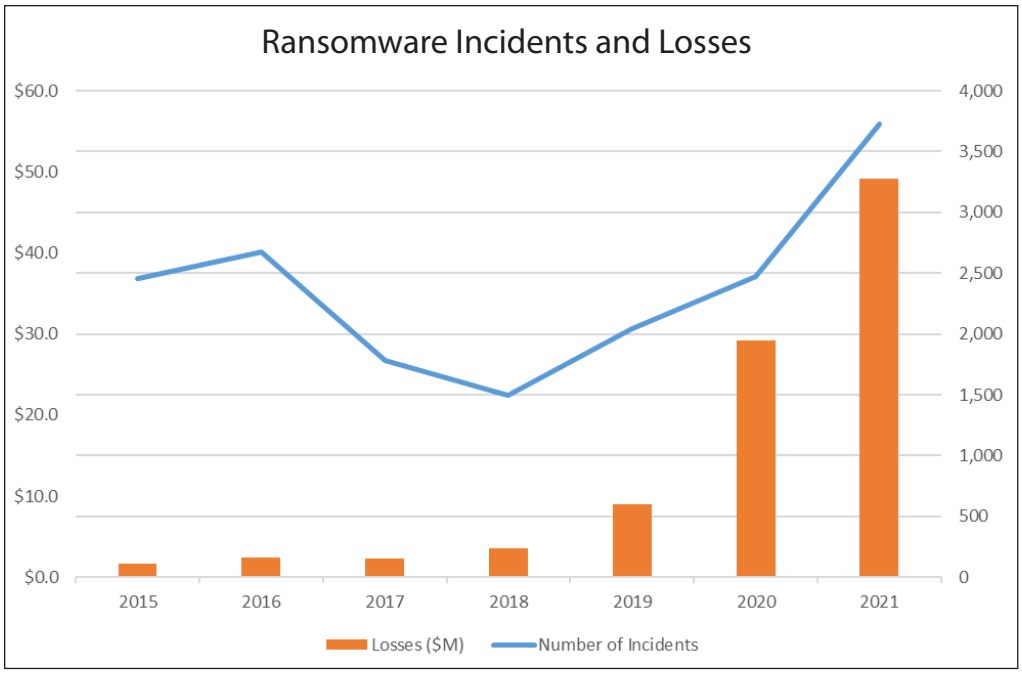
## Does paying the ransom work?

It is estimated that recovery keys are only effective 20% to 50% of the time and there still are rebuilding costs.[12] According to one ransomware specialty firm, ransom paid to delete stolen data is not always successful. Victims have been re-extorted weeks later, or data has been leaked after ransom was paid.[13]

## Insurance industry outlook

Insurance companies must respond to the increasing frequency and severity of ransomware attacks. The FBI's Internet Crime Complaint Center (IC3) reported 1,493 victims with $3.6 million in loss for 2018 and 2,047 complaints with adjusted losses over $8.9 million for 2019.[14] In 2020 and 2021, ransomware attacks and costs increased significantly, with 2,474 complaints in 2020 and 3,729 incidents in 2021.[15] Average losses increased from $2,426 per complaint in 2018 to $13,196 in 2021. [16]The following graph shows the number and cost of ransomware attacks reported to the IC3 in the years 2015 through 2021.

**Figure 10**




12 "Don't Pay Cyber Ransoms, Officials Warn"; op. cit.
13 "Ransomware Demands Continue to Rise"; CoveWare blog; Nov. 4, 2020.
14 FBI Internet Crime Reports for 2018 and 2019.
15 FBI Internet Crime Report for 2021
16 FBI Internet Crime Reports for 2018 and 2021

As concerning as these trends are, costs may be underreported. The IC3 ransomware costs data do not include estimates of lost business, time, wages, files, equipment, or any third-party remediation services acquired by a victim and only includes what victims report to the FBI via the IC3.[17] Company culture can determine what cybercrimes are reported. A company may underreport, or not report at all given concerns with potential reputational risk. Current OFAC guidance may deter reporting if the company decides to pay a ransom due to potential civil penalties, although the adjusted guidelines clarify that factors such as compliance with law enforcement may mitigate the impact to a company for reporting a cyber event.

Moody's Investors Services Inc. reports that the surge in ransomware is increasing cyber insurance prices, reducing limits and raising attachment points.[18] Marsh reports cyber insurance price increases of over 100% in the first quarter of 2022 for the U.S. and U.K., with many insureds accepting retention increases to mitigate increasing costs.[19] Insurance companies offering ransomware coverage may require that the insured make "every reasonable effort" not to reveal that they have this coverage.[20] Another way to limit costs is to require pre-approval before paying any ransom.[21] While insurance policies may not directly pay a ransom, some policies will reimburse insureds that choose to do so.

## Conclusion

Corvus, a cyber insurance firm, noted a decrease in claims frequency and severity for ransomware claims in the fourth quarter of 2021 and the first quarter of 2022.[22] Corvus notes that part of the decrease can be attributed to insurance underwriting, which promotes and often requires insureds to practice good cyber hygiene. However, ransomware is not going away anytime soon. Understanding the basics of ransomware is the first step in equipping companies and insurers to underwrite, price, and manage this cyber risk effectively. Insurers can continue providing guidance to their policyholders to help prevent attacks as well as how to respond after an attack.

17 *Internet Crime Report*; FBI; 2018 (page 20).
18 "Cyber insurance prices increase on ransomware claims: Moody's"; *Business Insurance*, Feb. 5, 2021.
19 "Global Insurance Market Index"; Marsh, 2022.
20 Insurance company rate filing.
21 Insurance company rate filing.
22 "Ransomware Claims Trending Downward, Insurance Firm Says"; Security Week, April 13, 2022.


AMERICAN ACADEMY OF ACTUARIES
1850 M STREET NW, SUITE 300, WASHINGTON, D.C. 20036
202-223-8196 | **ACTUARY.ORG**