

NetDiligence®

2020 Spotlight on

Ransomware

BASED ON THE
2019 CYBER CLAIMS STUDY

SPONSORED BY



RSM

**COZEN
O'CONNOR**



Introduction

Imagine being shut down for two weeks, after paying a ransom, discovering that your backups were also corrupted, or receiving demand letters alleging breach of contract by clients due to the ransom of your third-party cloud provider.

Welcome to the reality of a ransomware attack.

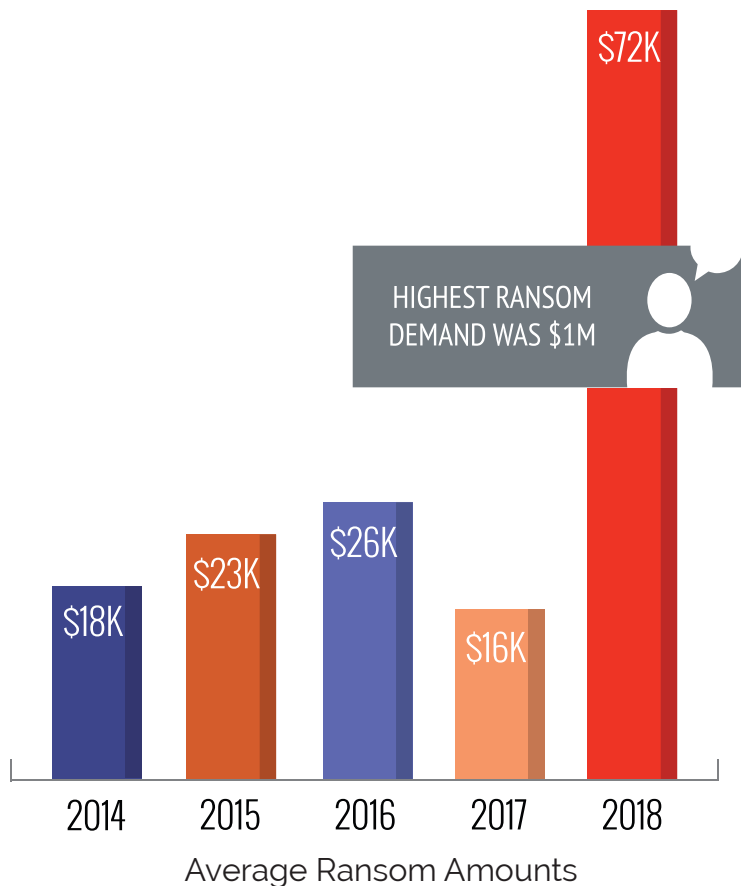
Threat actors use infected web portals, kiosk accounts, email phishing, and attachments to accomplish their objectives. They hold websites, laptops, PCs, networks, servers, backup systems and entire phone systems for ransom. Weapons include viruses, malware, and even pay-per-use "Ransomware as a Service" (RaaS) portals.

Since the end of 2017, the frequency and cost of ransomware events have been increasing sharply. Ransomware is now a significant headache for organizations of all sizes and in every sector. Because many victims have cyber insurance coverage, ransomware claims have become a leading cause of loss for the cyber insurance industry.

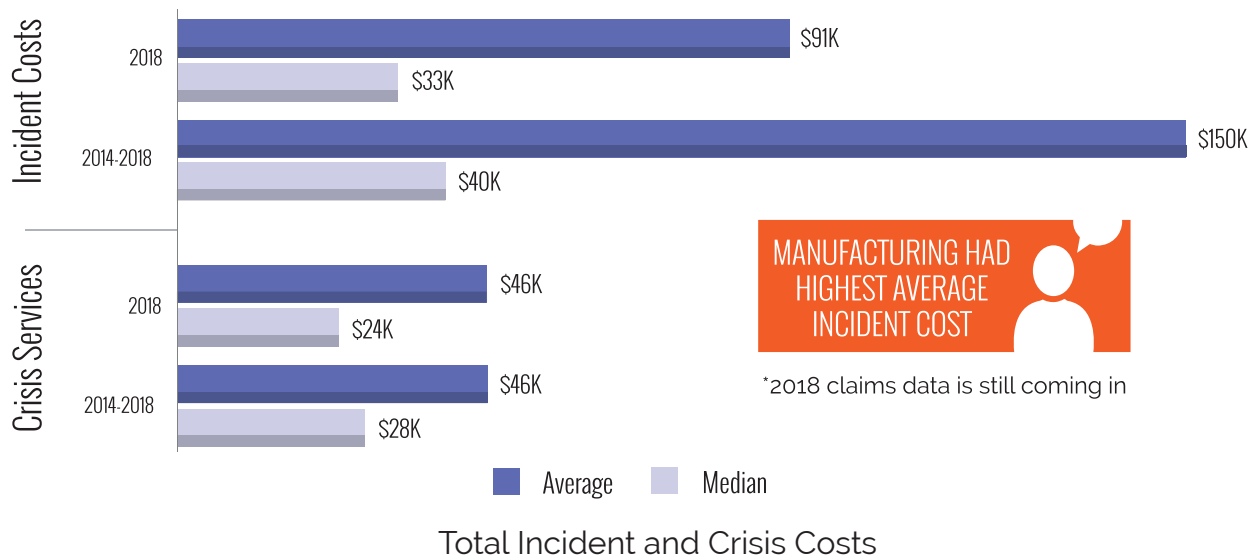
This *Spotlight on Ransomware* report is based on an analysis of 478 ransomware claims from the NetDiligence® dataset, dated 2014-2018, as well as information from public sources for ransomware events occurring in 2019.

Key Findings

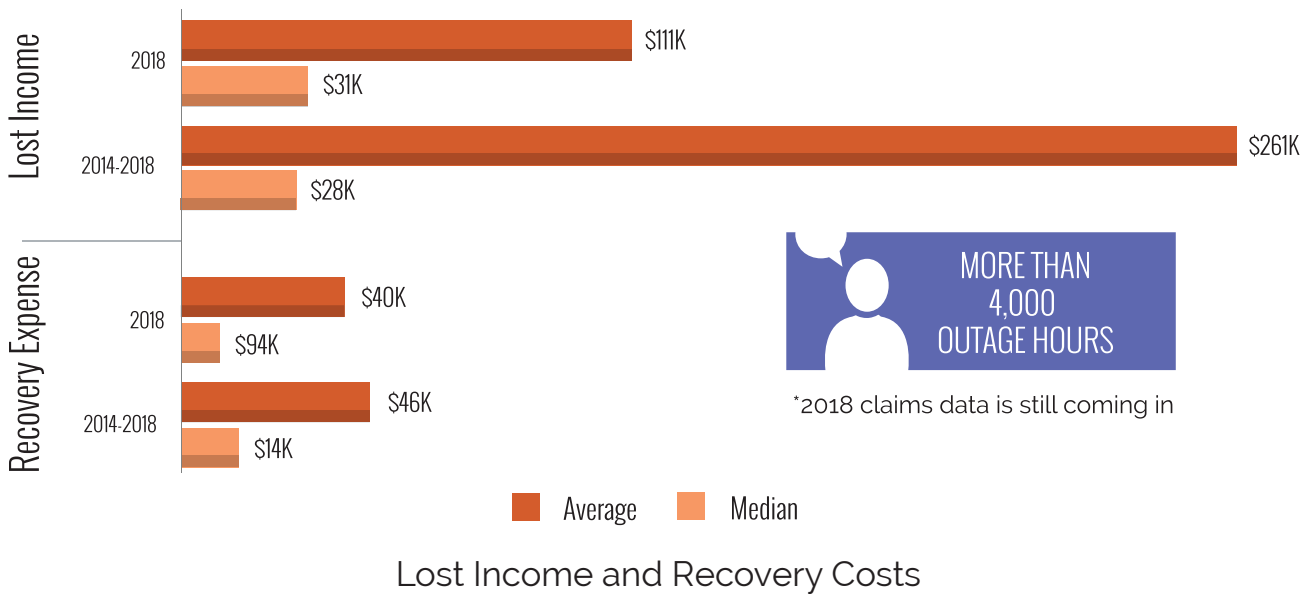
Ransom amounts are climbing



Costs are increasing*



Effects of business interruption are worsening*



Incident Costs with Ransom Paid and Not Paid

Despite public statements from the FBI and other law enforcement organizations, there is a growing trend for victims to pay ransoms quickly and get back to normal operations. The NetDiligence data bears this out: the average incident cost when a ransom was paid was much lower than when a ransom was not paid (\$111K vs. \$188K).

Just over half the cost of a ransomware event can be attributed to business income loss. Thus, from a financial perspective, it makes sense to minimize downtime, as well as to quickly mitigate the risk of brand damage, breach of contract issues, and other costs that may be hard to quantify but nonetheless are very real.

Number of Claims and Costs

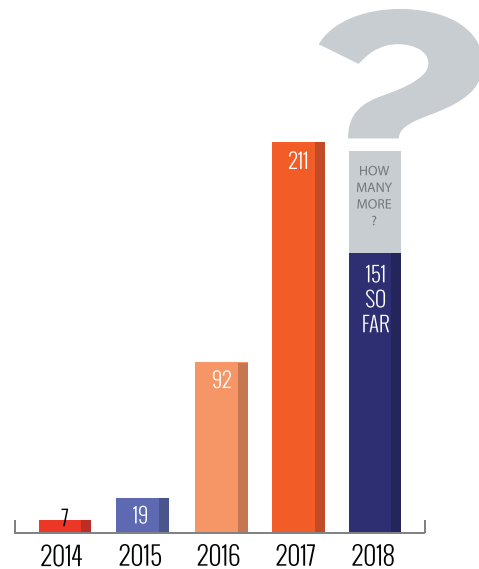
The number of ransomware claims in the dataset has increased dramatically over the past 5 years: 6 in 2014, 19 in 2015, 92 in 2016, 210 in 2017, and 151 so far in 2018. We anticipate seeing this trend continue in 2019.

Please see *The Cybercrime Explosion*¹, a report from the Insurance Industry Cybercrime Task Force, sponsored by NetDiligence, in which multiple industry experts report seeing multimillion-dollar payouts on a regular basis.

We see similar increases in ransomware incident costs over the same time period. Average incident costs have increased from \$35K in 2014 to \$209K in 2017. For 2018 (partial year) the average was \$91K. We expect this number to increase as we collect additional data points in 2020 and 2021.

For the first time, we have seen ransom demands at the \$1M mark, one larger than \$1M (Education) and one approximately \$900K (Professional Services).

Ransomware claims are skyrocketing



Number of Ransomware Claims

Business Sectors



Ransomware affected practically every sector.

Healthcare (N=166) and Professional Services (N=106) had the largest number of ransomware-related claims in the five-year period 2014-2018.

Education (\$170K) and Technology (\$86K) had the highest average ransoms paid.

Manufacturing (\$707K) and Technology (\$280K) experienced the highest total incident costs.²

¹ <https://netdiligence.com/portfolio/insurance-industry-cybercrime-task-force/>

² Based upon only two claims, the Entertainment sector had a slightly higher average breach cost (\$299K) than the Technology sector. Because the Technology sector average was based upon 16 claims, we chose to rank it second.

**NETDILIGENCE® CYBER CLAIMS STUDY
SPOTLIGHT ON RANSOMWARE**

Ransomware Claims by Business Sector - 2018

Sector	Claims	Range	Average	Median
Education	2	10K-1.2M	580K	580K
Financial Services	7	24K-236K	87K	38K
Healthcare	60	1K-575K	51K	28K
Hospitality	2	23K-60K	41K	41K
Manufacturing	9	3K-251K	98K	43K
Non-Profit	3	10K-54K	27K	17K
Professional Services	24	4K-2.6M	168K	33K
Public Entity	4	5K-102K	53K	53K
Restaurant	1	97K-97K	97K	97K
Retail	11	5K-380K	79K	54K
Technology	8	10K-547K	217K	156K
Transportation	4	5K-177K	54K	16K

Table 1

Ransomware Claims by Business Sector - 2014-2018

Sector	Claims	Range	Average	Median
Education	17	10K-1.2M	146K	54K
Energy	5	11K-132K	44K	28K
Entertainment	2	74K-525K	299K	299K
Financial Services	24	5K-305K	64K	36K
Healthcare	166	1K-6.6M	145K	35K
Hospitality	4	23K-60K	42K	43K
Manufacturing	31	3K-20M	707K	39K
Media	2	5K-75K	40K	40K
Non-Profit	14	2K-84K	34K	18K
Professional Services	106	3K-2.6M	88K	38K
Public Entity	22	5K-328K	68K	61K
Restaurant	2	47K-97K	72K	72K
Retail	23	5K-380K	71K	54K
Technology	16	10K-2M	280K	118K
Telecommunications	1	17K-17K	17K	17K
Transportation	11	5K-790K	141K	90K

Table 2

2019

The NetDiligence dataset does not yet contain claims for 2019 (we are currently collecting data for the 2020 report). For this reason, we have looked to the public record.

2019 has been an increasingly active and costly year for organizations and insurers. Ransom amounts have skyrocketed into the millions of dollars. City and state governments have been especially hard hit. Since suffering an attack in 2018, the City of Atlanta has spent over \$17M in recovery and mitigation costs. The City of Baltimore has spent over \$18M. Twenty-two local governments in Texas have spent in excess of \$12M.

In the private sector, the Norwegian producer of aluminum, Norsk Hydro, has incurred over \$60M in recovery and mitigation costs. The Danish hearing aid manufacturer, Demant, has spent over \$80M. At the time of this writing, the international currency exchange company, Travelex, is shut down by ransomware. Travelex is one to watch as the criminals have increased the ransom demand from \$3M to \$6M recently.

Emerging Issues

In closing, we would like to highlight two important issues. The first concerns the rising costs of ransomware events for both insurers and insureds. Not only are ransom amounts increasing, they are "becoming disproportionate to the size of targets."³ As a result, insurers are increasing rates for cyber insurance coverage for clients of all sizes. In addition to charging higher premiums, some insurers are looking to share the costs with their insureds. One leading cyber insurer has suggested that higher-risk victims of ransomware might be required to pay 20-30% of the cost of an event as an incentive to improve their defenses.⁴

Non-affirmative coverage is another issue of continuing concern to insurers. While not new, non-affirmative coverage is being discussed by the media due to a recently decided court case.⁵ In this case, a federal

judge ruled that a ransomware attack had resulted in "actual damage" to property, and that the defendant insurance company was therefore obligated to provide coverage under the terms of the insured's traditional (non-cyber) business owner's policy. One case doesn't make a trend but the court's ruling in this matter is bound to attract the notice of insurers.

Conclusion

Ransomware affects organizations of all sizes and in all sectors. As evidenced by the number of healthcare and public entities that have been attacked, threat actors feel no moral constraints about whom they go after and whether they put peoples' lives at risk.

Unfortunately, this scourge of the interconnected world is not likely to go away anytime soon. From the attackers' point of view, it's a business model that works. The value of credit card and personal data for sale on the dark web is very low. So, why take the time to reconnoiter and model a victim in order to steal data when all you have to do is lock down systems and collect ransoms? By one estimate, over the past few years, a single gang in Eastern Europe has collected \$2B in ransoms.

We don't mean to paint a picture that is entirely black. Technologies are being created and evolving to counter these kinds of threats, for example next-generation endpoint malware protection that reacts to and prevents suspicious behavior, as opposed to a static virus signature. And, as always, good employee training is the backbone of good defense. For more detailed anti-ransomware tips, please see **Must-Have Ransomware Safeguards**, a NetDiligence call-to-action paper inside the eRiskHub®.

Note on Methodology

Our data collection, analysis, and reporting methodology are described in detail in the full 2019 NetDiligence Cyber Claims Study, available at <https://netdiligence.com/portfolio/cyber-claims-study/>.

³ Kelly Castriotta, Allianz SE, quoted by Suzanne Barlyn, *Insurance Journal*, January 22, 2020, "Ransomware Exposure Driving up Cyber Insurance Costs."

⁴ *Ibid.*

⁵ National Ink & Stitch LLC v. State Auto Property & Casualty Insurance Co., case number [1:18-cv-02138](#), U.S. District Court for the District of Maryland.

Thank You to Our Sponsors

RSM US

RSM US LLP is the leading provider of audit, tax and consulting services focused on the middle market, with nearly 11,000 people in 87 cities and four locations in Canada. It is a licensed CPA firm and the U.S. member of RSM International, a global network of independent audit, tax and consulting firms with more than 41,000 people in 116 countries. RSM uses its deep understanding of the needs and aspirations of clients to help them succeed. For more information visit <https://rsmus.com/>



About Cozen O'Connor

Cozen O'Connor has a multidisciplinary team of highly skilled and nationally regarded attorneys who focus on all aspects of privacy and data security counseling and litigation. We help companies protect data, comply with regulations, and respond to investigations and litigation. Ranked among the top 100 law firms in the country, Cozen O'Connor has more than 750 attorneys in 27 cities across two continents. A full-service firm with nationally recognized practices in litigation, business law, and government relations, our attorneys have experience operating in all sectors of the economy. cozen.com



About NetDiligence®

NetDiligence® is a leading provider of Cyber Risk Readiness & Response services. We have been providing cyber risk management services and software solutions to the cyber insurance industry, since 2001. Our cyber conferences and advisory groups serve as platforms for insurers, legal counsel, and technology specialists to exchange knowledge. This community of experts serves as the vanguard in the fight against cyber losses. We listen and learn from them. That's why our services support our insurance partners and their policyholders both proactively for cyber readiness and reactively for incident response.

and predictable costs. This Software-as-a-Service (SaaS) offering provides tools and resources to help clients understand their exposures, harden their cyber defenses, and respond effectively to minimize the effects of breaches on their organizations. Our mobile-friendly, flexible platform can be branded, customized and delivered to any domain. Plus, it's scalable! Start small and increase your license as you grow. You can also add content for other geographic regions as you expand globally.

QuietAudit® Cyber Risk Assessments

NetDiligence's QuietAudit® Cyber Risk Assessments give organizations a 360-degree view of their people, processes and technology, so they can reaffirm that reasonable practices are in place; harden and improve their data security; qualify for network liability and privacy insurance; and bolster their defense posture in the event of class action lawsuits. We offer a variety of consultant-led assessments and vulnerability scan services to meet the unique needs of small, medium and large organizations.

Breach Plan Connect®

Breach Plan Connect® provides step-by-step guidance to help companies develop a comprehensive, yet actionable, breach response plan *for senior managers*. The software comes loaded with a customizable plan designed to help management oversee and coordinate the organization's response to a cyber event. It includes a partner mobile app so that the response team can communicate even if the company's systems have been compromised.

eRiskHub®

The eRiskHub® portal, powered by NetDiligence, is an effective way to help both insurers and their clients combat cyber losses with minimal, controlled

Contact Us

For more information, visit us at netdiligence.com or email us at management@netdiligence.com.

