

# NetDiligence®

2018  
CYBER  
CLAIMS  
STUDY

2019 Spotlight  
PUBLIC  
ENTITIES

SPONSORED BY

**AIIClear ID**

**RSM**

# Introduction

NetDiligence® is pleased to release this spotlight report on cyber claims within the Public Entity sector. We examined the overall costs, key causes of loss, and other important areas of concern for the five-years 2013-2017, as well as 2017 separately.

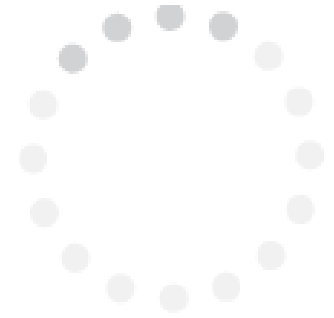
Although claims from Public Entities constitute a small percentage (3%) of overall claims in our dataset, the number of claims has doubled each year since 2015, from 5 to 10 to 20 in 2017.

Public Entities include the following types of organizations:

- Municipalities and Townships
- Social Services Organizations
- Police Departments
- Prisons
- Museums and Zoos

As you review the findings in this report, please keep in mind that the vast majority of the data breach claims in this study involved smaller organizations. As a result, our median and average costs tend to be lower than the breach costs reported in more general studies.

Please also note that throughout this report we use the term “crisis services” as an umbrella category for emergency breach response services, including Breach Coach® (legal) guidance, forensics, notification and credit/ID monitoring.



## Key Findings

- The five-year average breach cost was \$78K; the 2017 average breach cost was \$77K.
- The five-year average cost for crisis services was \$63K; the 2017 average cost for crisis services was \$65K.
- For the five-year period, crisis services costs (as a percentage of total breach costs) were much higher for Public Entities (81%) than for organizations overall (51%).
- 76% of claims included forensics costs – \$39K was the five-year average.
- 95% of claims included costs for legal guidance/Breach Coach® – \$21K was the five-year average.
- 55% of claims exposed sensitive records. The five-year:
  - Average breach cost was \$87K.
  - Average number of records exposed was 6,740.
  - Average per-record cost was \$246.
  - Median per-record cost was \$107.
- 45% of claims were for “recordless” breaches. The five-year average breach cost for “recordless” claims was \$67K.
- Criminal activity accounted for 84% of claims and had an average breach cost of \$88K.
- Non-criminal activity accounted for the remaining 16% of claims and had an average breach cost of \$27K.

# Discussion

## Causes of Loss

Causes of loss included hacking, malware/virus, rogue employees, ransomware, business email compromise (BEC), staff mistakes, and programming errors. The top four, by cost, were:

Cause of Loss	Claims	Average Breach Cost
Hacking	7	\$70K
Malware/Virus	3	\$59K
Rogue Employee	3	\$54K
Ransomware	15	\$21K

Ransomware accounted for 39% of Public Entity claims in our dataset. Not all ransomware claims specified the ransom amount, but for those that did, ransoms ranged from \$5K to \$12K (\$8K average). Forensics and business recovery accounted for 90% of the cost of ransomware events.

Overall, the claims in our dataset describe events that were contained to a single user on a single device that was not networked. The average breach cost for these incidents was \$71K. For claims in which the data could be restored from backup, the average breach cost was \$59K.

## Insiders vs External Parties

Insiders accounted for 34% of claims, with the most damaging attributed to rogue employees/malicious insiders. The five-year average breach cost for malicious insider events was \$98K, of which \$59K was for crisis services. The average five-year breach cost for unintentional insider events was \$66K, of which \$45K was for crisis services.

The remainder of Public Entity claims (66%) were caused by external parties. The five-year average breach cost for externally-caused events was \$82K, of which \$72K was for crisis services.

Municipalities, Townships and Police Departments suffered the greatest losses for events in which there was definitive proof that the external party was tied to a foreign IP address. These criminal actors targeted databases containing arrestees, victims and witnesses. Even though these attacks were unsuccessful in the exfiltration of confidential data due to the organizations' network configurations, the attacks did result in damage to emergency management systems.

## Protected Information

Claims involving the theft or exposure of protected information (PII, PHI, and W-2 data) accounted for 53% of claims for the five-year period. The average breach cost for these events was \$88K, of which \$70K was for crisis services.

One important finding involves the exposure of jail and prison inmates' personal information. Our database contains multiple claims of this type. For the five-year period, the average number of records exposed was 18K and the average cost per record was \$244. The average breach cost was \$150K, of which \$147K was for crisis services.

To quote *The Man with the Stolen Name* 05.15.2018 ([www.themarshallproject.org/2018/05/14/the-man-with-the-stolen-name](http://www.themarshallproject.org/2018/05/14/the-man-with-the-stolen-name)):

*"The incarcerated, it turns out, are easy marks for identity thieves and, as that crime grows—up 16 percent last year—more prisoner Social Security numbers and names are being stolen for tax fraud and other purposes. With limited or no access to computers, credit checks or social media, prisoners may not discover that their identities have been stolen until after they are released."*

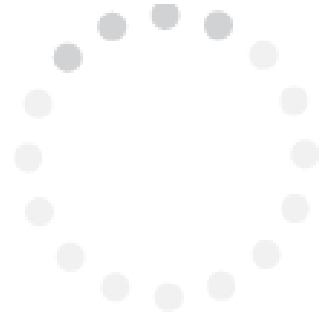
## Conclusion

In the past, Public Entities may not have fully appreciated the value of the data they hold and therefore did not regard themselves as a target for cyberattacks. But a mindset of "Who'd be interested in us?" is no longer viable. Over the past few years, cyberattacks in Atlanta and other locales have clearly demonstrated this.

While Public Entities may be at a budgetary disadvantage compared to commercial enterprises, it is imperative that they understand their obligation to protect the privacy of their citizens and work to improve their cybersecurity.

## A Note on Methodology

Our data collection, analysis, and reporting methodology are described in detail in the full 2018 NetDiligence® Cyber Claims Study.





## About NetDiligence®

NetDiligence® specializes in Cyber Risk Readiness & Response services. With more than 15 years of experience in cyber, NetDiligence is an award-winning provider of innovative cyber risk management software and services to the insurance industry, including [QuietAudit® Cyber Risk Assessments](#), the [eRiskHub®](#) cyber risk management portal, and [Breach Plan Connect®](#) software-as-a-service (SaaS) that helps companies develop an effective data breach response plan. NetDiligence publishes an annual [Cyber Claims Study](#) and hosts annual [Cyber Conferences](#) in Philadelphia, Santa Monica, Toronto, London and Bermuda.

### Contact Us

For more information about NetDiligence® or any of our service offerings, please visit us at [NetDiligence.com](https://netdiligence.com), email us at [management@netdiligence.com](mailto:management@netdiligence.com), or call us at 610.525.6383.

