NetDiligence®

PUBLIC ENTITIES

2021 SPOTLIGHT REPORT

OUR SPONSORS

RSM

experian.

GUIDEWIRE CYENCE

Beckage
Legally Focused. Technology Driven.

Table of Contents

Introduction

NetDiligence® is pleased to release its second Spotlight Report on the cyber claims experience in the Public Entity sector. Using a dataset of 249 claims, we examined the demographics, overall costs, key causes of loss, and other important areas of concern for the five -years 2016--2020, as well as 2020 separately.

Although claims from Public Entities constitute a small percentage (4%) of overall claims in our dataset, the number of claims has increased dramatically from 20 in 2016 to 50 or more in each year since then.

Key Findings

- The average incident cost was $120K (2016-2020), up from $78K in the 2019 report (2014-2018); in 2020, the average incident cost was $136K.
- The average 5-year cost for crisis services was $116K, up from $63K in the 2019 report; in 2020, the average cost for crisis services was $76K.
- Crisis Services costs (as a percentage of total incident cost) were much higher for Public Entities (97%) than for organizations overall (79%).
- Criminal activity accounted for 72% of claims; the average incident cost was $145K.
- Non-criminal activity accounted for the remaining 28% of claims; the average incident cost was $50K.
- Ransomware was the leading cause of loss by far:
  - 32% of all Public Entity claims involved Ransomware.
  - The average incident cost was $157K
  - The aggregate loss was over $11M

The data for Public Entities in the NetDiligence dataset has been collected from state and local governmental entities and agencies. To the best of our knowledge, no federal departments or agencies are represented in the data.

Public Entities in this report include the following types of organizations:

- Counties and county agencies (32%)
- Municipalities and townships (4%)
- Social Services organizations (15%)
- Child and Youth Services agencies (3%)
- Law Enforcement agencies (N=1%)
- Jails and prisons (1%)
- Other or not specified (44%)

Notes:

Findings are for the five-year period 2016-2020, unless otherwise noted.

As you review the findings in this report, please keep in mind that most of the cyber claims in this study involved smaller organizations. As a result, average costs tend to be lower than incident costs reported in more general studies.

Demographics and Overall Findings

Claim Volume

Since 2017, the number of Public Entity claims that NetDiligence received has been fairly constant, ranging from 44 to 57 per year (2017-2020).

Percentage of Claims by Year

(N=222)

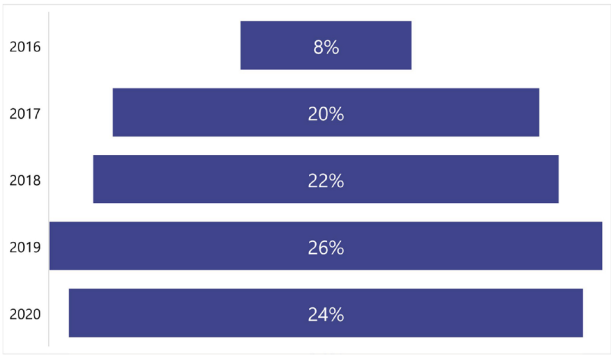

Figure 1

Organization Size

As was noted above, most of the claims in the dataset come from smaller organizations. The average Public Entity was estimated to have annual revenues of $123M (N=88), ranging from $50K to over $10B .

When classified by revenue size categories, over half of Public Entity claims came from organizations with less than $300M in annual revenues[1].

Percentage of Claims by Size

(N=222)

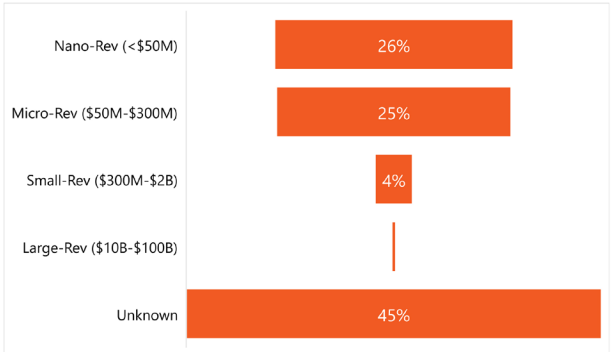

Figure 2

[1] *One outlier – a $10B organization was removed from the calculation because it significantly skewed the average.*

Average Incident Cost

The average cost of an incident at a Public Entity has varied quite a bit since 2016. After a dip in 2018, these costs increased significantly in 2019 and 2020.

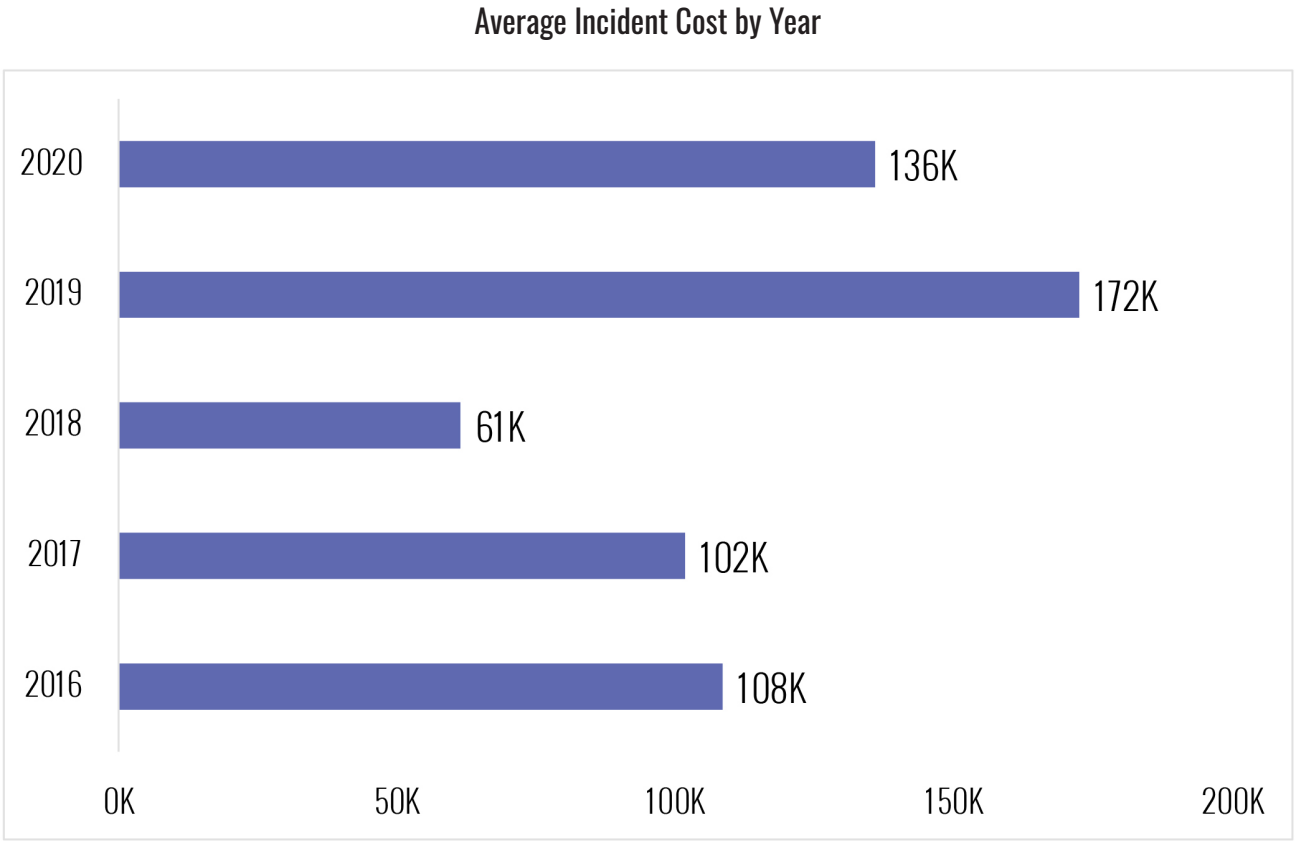

Figure 3

Causes of Loss

Public Entities experience cyber losses for many reasons, primarily because of the actions of criminals (72%), but also because of staff mistakes, programming errors, etc. The top four causes of loss for the five-year period were Ransomware, Hackers, Staff Mistakes, and Business Email Compromise. For the complete list of Causes of Loss, see the Appendix

Top 4 Causes of Loss

Number of Claims, Total Incident Cost, Percentage of Overall Incident Cost

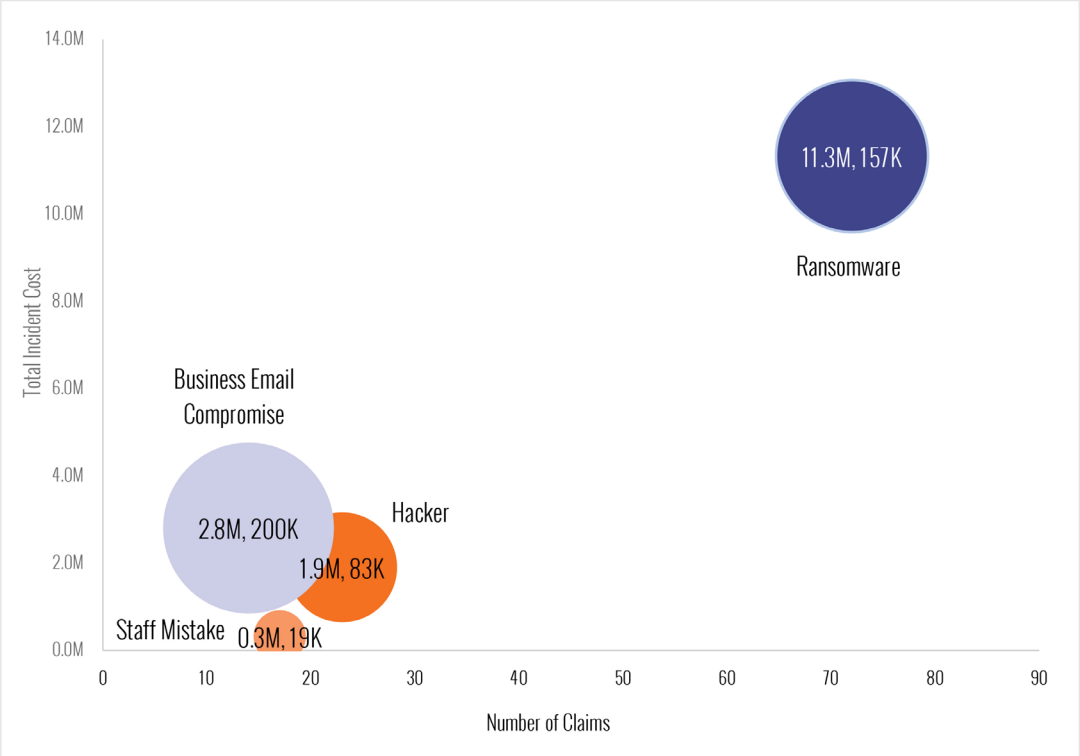

Figure 4

During 2016-2020, Ransomware claims accounted for 32% of the claims in the dataset. Not all Ransomware claims specified the ransom amount, but for those that did (N=18), ransoms ranged from $2K to $800K ($249K average). For these claims, the average incident cost was $358K. In 2020 (N=6), the corresponding numbers were: average ransom=$421K; average incident cost=$480K.

Ransoms were not paid in a small number of claims (N=7). In these cases, systems were either restored from backups, or redundant systems existed. The incident cost for these events was much lower than for other Ransomware events, ranging from $15K to $52K with an average of $32K.

Cyber incidents attributed to the mistakes and negligence of third-party vendors accounted for about 7% of the claims in the dataset. For the five-year period, these claims averaged $269K, ranging from $9.5K to $2.5M. In only three third party claims were the vendors identified: BlackBaud, Solar Winds, and Tyler Technologies.

Claims attributed to Insiders and Rogue Employees accounted for less than 2.5% of cyber incidents in the dataset. Average incident and crisis services costs can be found in the Appendix.

Types of Data

The top four types of data involved in cyber incidents at Public Entities were Files – Critical[2] , PII, Email – Unspecified, and Non-Card Financial data.

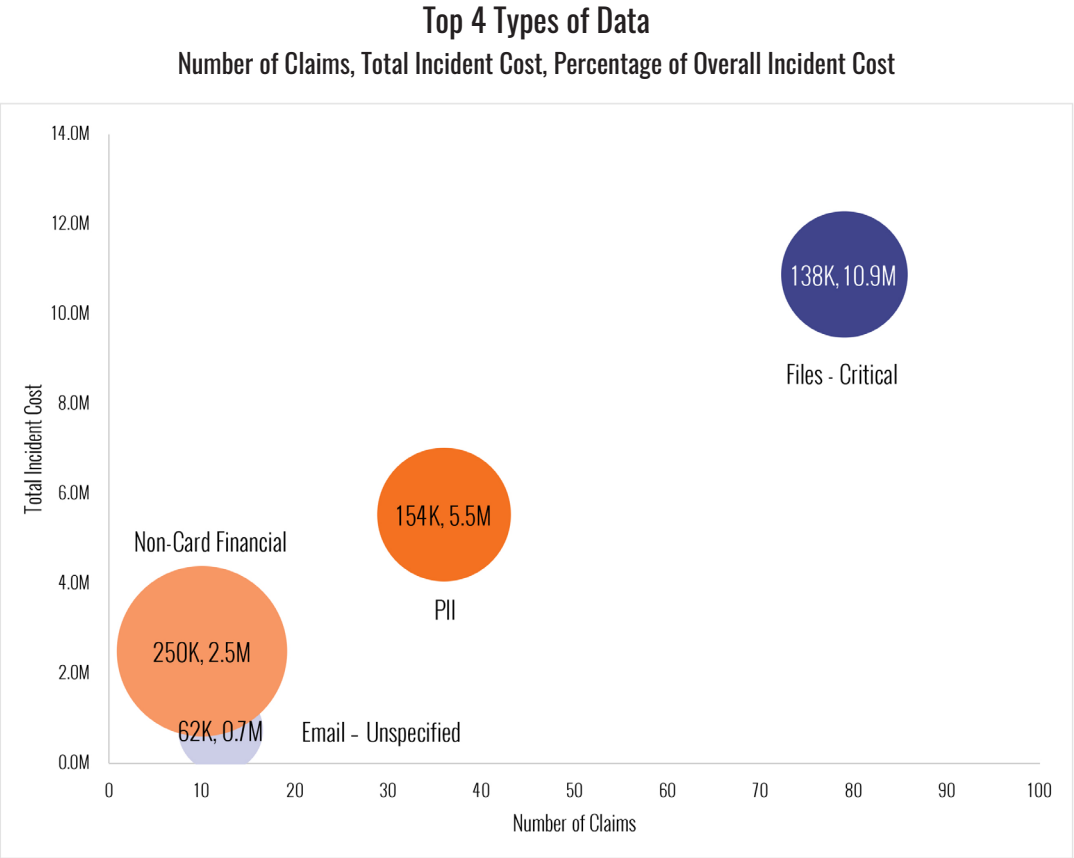

Figure 5

The full table of incident and crisis services costs for each type of data can be found in the Appendix.

In the 2019 report, one important finding involved the exposure of jail and prison inmates' personal information. While this no doubt continues to be a problem, the dataset contains only three claims involving jails or prisons, so no analysis was performed.

[2] *Files – Critical: this category was created several years ago to capture events where systems and/or networks were locked down by ransomware or DDoS attacks. In these types of events, it is often neither possible nor relevant to assign a meaningful type of data such as PII, PHI, etc.*

Conclusion

Cyber incidents at Public Entities often make for big headlines, big headaches, and big losses. Even more often, these events go unreported to the public. While it is impossible to know how many of the claims in the NetDiligence dataset came from publicly disclosed incidents, it is probably fair to guess that the number is very small.

It is well known that Public Entities suffer from several disadvantages when compared to private entities:

- The "Who would be interested in us?" mentality is still very much alive and well, especially in smaller counties and municipalities.
- Since Public Entities are heavily dependent on tax receipts for their operating revenues, it is sometimes difficult to allocate the financial resources necessary to implement effective security programs.
- Given the shortage of skilled cybersecurity personnel and the relatively high salaries that experienced practitioners command, Public Entities are often locked out of the market for the best people.

Despite these disadvantages, it is imperative that Public Entities understand their obligation to protect the security of their systems and the privacy of their citizens.

Methodology

Our data collection, analysis, and reporting methodology are described in detail in the full 2021 NetDiligence® Cyber Claims Study.

Our Sponsors

About RSM

RSM is the leading provider of audit, tax and consulting services focused on the middle market, with nearly 13,000 professionals in 83 U.S. cities and four locations in Canada. It is a licensed CPA firm and the U.S. member of RSM International, with 48,000 people in more than 120 countries. For more information, visit https://rsmus.com/.

About Guidewire

Guidewire is the platform P&C insurers trust to engage, innovate, and grow efficiently. We combine digital, core, analytics, and AI to deliver our platform as a cloud service. More than 400 insurers, from new ventures to the largest and most complex in the world, run on Guidewire. For more information, contact us a info@guidewire.com.

About Experian® Data Breach Resolution

Experian® Data Breach Resolution, powered by the nation's largest credit bureau, is a leader in helping businesses prepare for a data breach via the proprietary Experian® Reserved Response program and also mitigate consumer risk following breach incidents. With more than nineteen years of experience, Experian has successfully serviced some of the largest and highest-profile data breaches in history. The group offers swift and effective incident management, notification, call center support and fraud resolution services while serving millions of affected consumers with proven credit and identity protection products. For more information, visit www.experian.com/databreach and follow us on Twitter @Experian_DBR.

About Beckage

Beckage is a women-owned law firm focused on technology, data security, and privacy. Our attorneys counsel clients on matters pertaining to data security and privacy compliance, litigation and class action defense, incident response, government investigations, technology intellectual property, and emerging technologies. Our lawyers are technologists, tech business owners, CISAs, CISOs, former regulators, and certified privacy professionals. Learn more at Beckage.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, both insurers and policyholders, since 2001.

Our Cyber Risk Summit conferences and our cyber advisory groups function as information exchange platforms for insurers, legal counsel, and technology specialists. 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.

Breach Response Solution with Mobile App

Breach Plan Connect® is a securely hosted solution designed to help senior managers plan for, oversee, and coordinate their organization's response to a cyber incident. Breach Plan Connect comes pre-loaded with a comprehensive incident response plan template that can be easily customized. It also includes a free mobile app for convenient access and alternative means of communication if company systems are compromised.

Risk Management Portal for Insurers

The eRiskHub® is a white-label cyber risk management portal that helps both insurers and their clients combat cyber losses. 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 a cyber incident. 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.

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 network vulnerability scans and consultant-led assessments that are tailored to meet the unique needs of small, medium, and large organizations in all business sectors. A variety of automated online self-assessment surveys are also available for underwriting loss control and vendor risk management.

On-Site & Virtual Cyber Programs

The leading networking events for the cyber industry, NetDiligence conferences are attended by thousands of cyber insurance, legal/regulatory, and security/privacy technology leaders from all over the world. Each event features programming curated by cyber professionals and focused on current and emerging concerns in the ever-changing cyber landscape. We traditionally host five on-site conferences per year, in Philadelphia, Santa Monica, Toronto, London, and Bermuda.

Contact Us

For more information, visit us at netdiligence.com, email us at management@netdiligence.com or call us at 610.525.6383.

NetDiligence®

Appendix

Data Tables

Incident Cost by Cause of Loss – 5 Years (2016-2020)

Cause of Loss	Claims	Average	Minimum	Maximum	Total
Business Email Compromise	14	200K	3K	1.4M	2.8M
Cyber Event - unspecified	11	121K	5K	560K	1.3M
Hacker	23	83K	4K	375K	1.9M
Legal Action	2	13K	5K	21K	27K
Lost/Stolen Laptop/Device	4	5K	0K	10K	18K
Malware/Virus	12	75K	4K	242K	905K
Negligence	1	5K	5K	5K	5K
Other	5	30K	2K	94K	148K
Paper Records	2	328K	5K	650K	655K
Phishing	13	85K	11K	338K	1.1M
Programming Error	4	725K	8K	2.5M	2.9M
Ransomware	72	157K	2K	1.0M	11.3M
Rogue Employee	5	62K	10K	151K	308K
Social Engineering	1	16K	16K	16K	16K
Staff Mistake	17	19K	2K	64K	319K
Theft of Hardware	2	14K	3K	25K	28K
Third Party	1	69K	69K	69K	69K
Unauthorized Access	1	20K	20K	20K	20K
Wire Transfer Fraud	5	195K	35K	505K	974K
Wrongful Data Collection	1	35K	35K	35K	35K
Unknown	26	66K	0K	612K	1.7M

Table 1

Average Crisis Services Cost by Cause of Loss – 5 Years (2016-2020)

Cause of Loss	Forensics	Notification	Monitoring	Legal Guidance	Total
Business Email Compromise	82K	6K	27K	44K	111K
Cyber Event - unspecified	50K	1K	0.3K	3K	54K
Hacker	39K	61K	31K	31K	116K
Legal Action	2K	5K	1K	8K	16K
Lost/Stolen Laptop/Device				0.3K	0.3K
Malware/Virus	32K	10K		25K	69K
Negligence				0.1K	0.1K
Other	10K	20K		20K	36K
Programming Error	1.1M	647K		57K	934K
Ransomware	53K	8K	3K	13K	132K
Rogue Employee	54K			5K	57K
Social Engineering	3K			8K	11K
Staff Mistake	5K	4K	4K	8K	13K
Third Party			69K		69K

Table 2

Incident Cost by Type of Data – 5 Years (2016-2020)

Cause of Loss	Claims	Average	Minimum	Maximum	Total
Email - unspecified	12	62K	3K	200K	742K
Files - Critical	79	138K	2K	1.0M	10.9M
Intellectual Property	1	63K	63K	63K	63K
N/A	7	159K	16K	351K	1.1M
Non-Card Financial	10	250K	3K	1.4M	2.5M
Other Non-Public Data	6	38K	7K	123K	231K
PCI	3	66K	35K	120K	197K
PHI	4	279K	6K	650K	1,114K
PII	33	162K	2K	2.5M	5.3M
User Credentials	3	174K	83K	230K	521K
W-2 Data	3	65K	30K	96K	195K
Unknown	61	61K	0.2K	612K	3.7M

Table 3

Average Crisis Services Cost by Cause of Loss – 5 Years (2016-2020)

Cause of Loss	Forensics	Notification	Monitoring	Legal Guidance	Total
Email - unspecified					
Files - Critical	50K			11K	132K
Intellectual Property					
N/A	37K	12K		9K	37K
Non-Card Financial	95K			42K	131K
Other Non-Public Data	26K			33K	50K
PCI	29K	6K	0.1K	28K	46K
PHI				6K	190K
PII	96K	82K	19K	26K	166K
User Credentials	91K	2K	60K	39K	170K
W-2 Data	20K	4K	46K	35K	62K
Unknown	30K	22K	0.4K	14K	42K

Table 4

Histogram

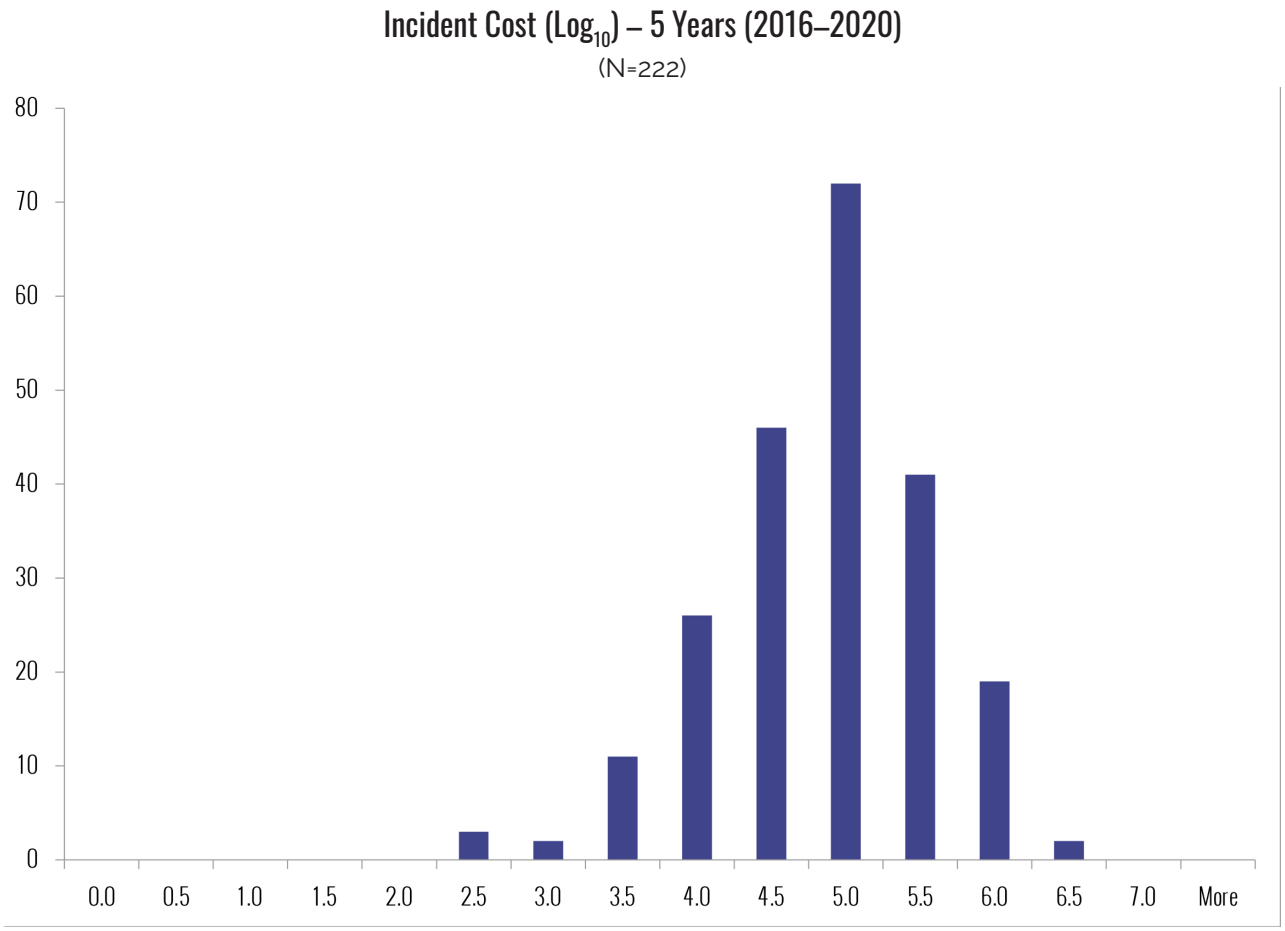

Figure 6

Box Plots

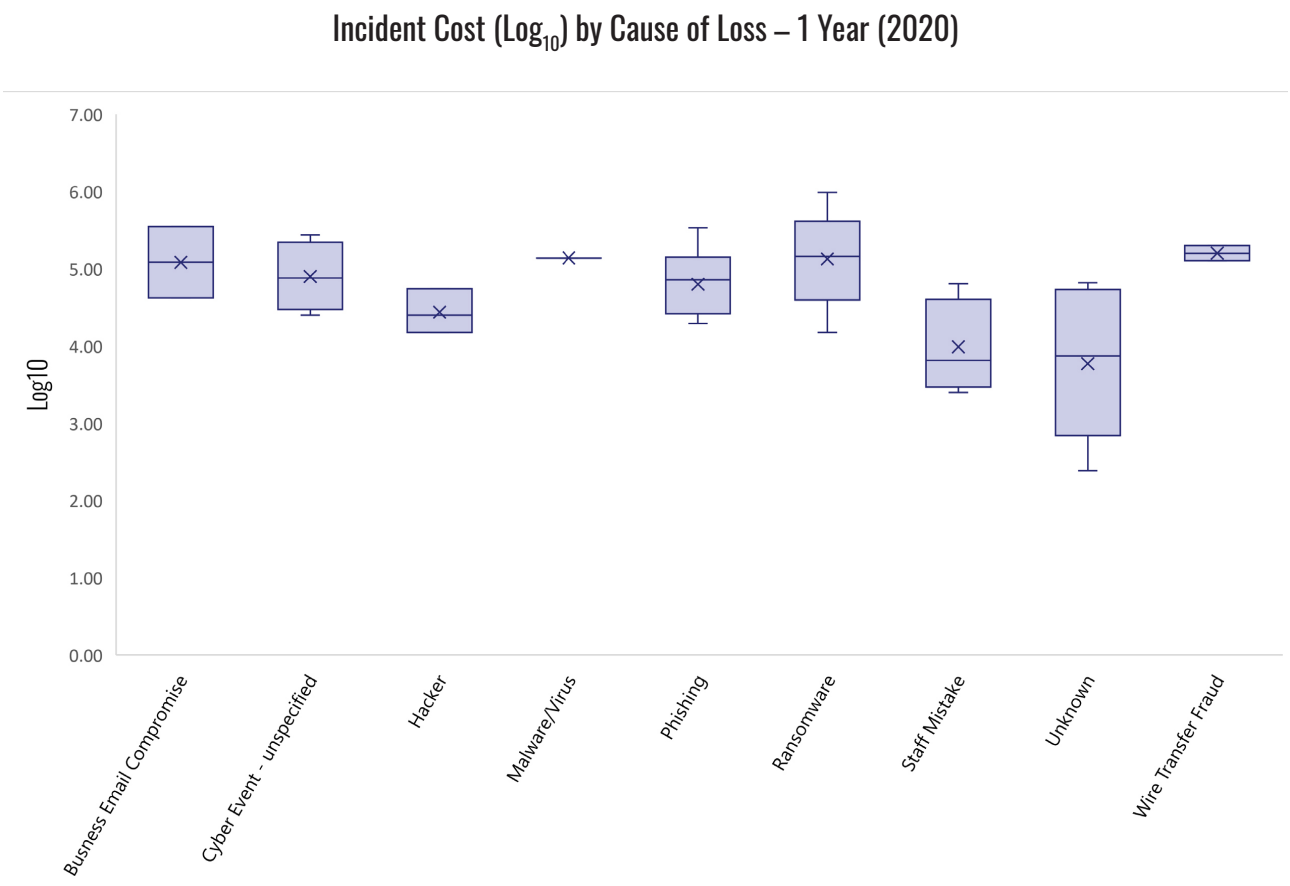

Figure 7

Incident Cost (Log_{10}) by Cause of Loss – 5 Years (2016–2020)

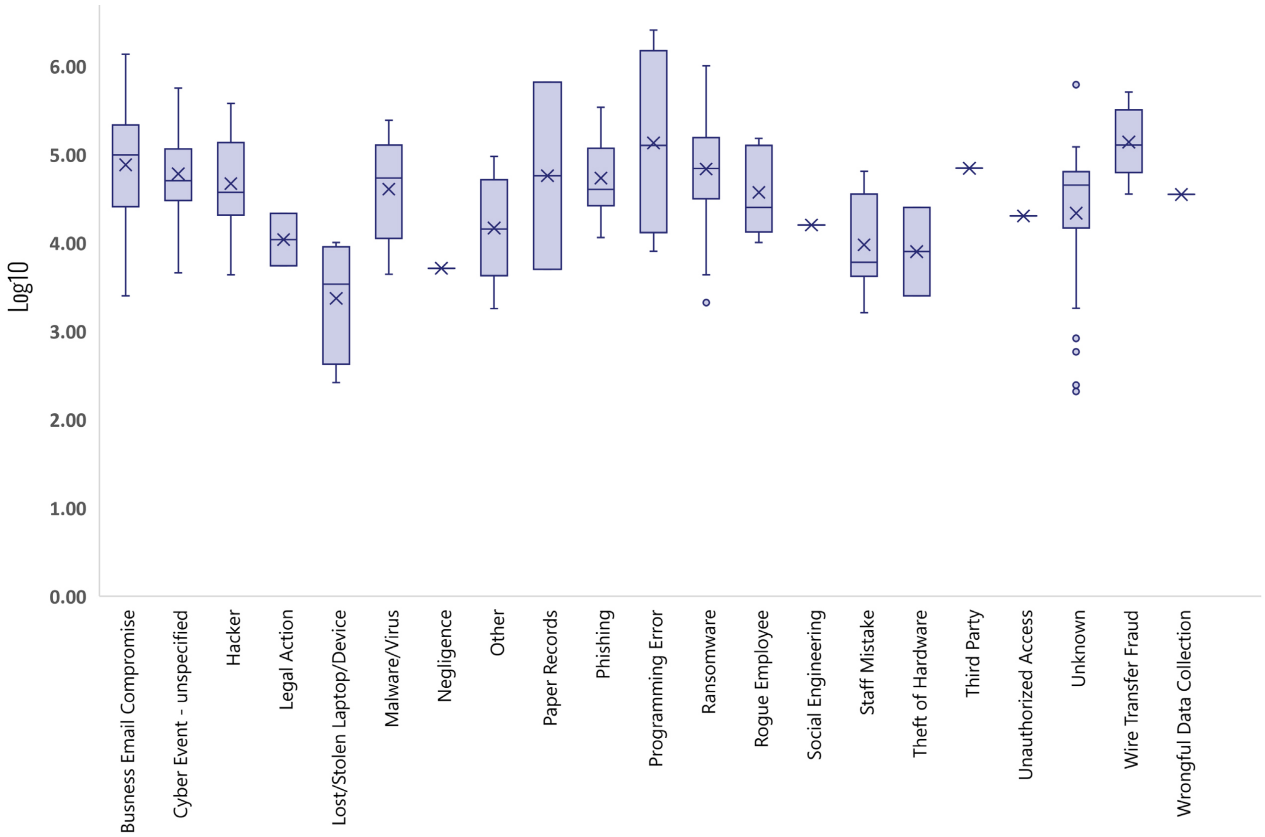

Figure 8

Percentile Tables

Incident Cost – 1 Year (2020)

(N=53)

Quartiles		
First	Min	244
	1.0%	419
	2.5%	654
	5.0%	1,410
	10.0%	4,050
	20.0%	18,657
Second	25.0%	25,000
	30.0%	25,001
	40.0%	39,816
Third	50.0%	62,476 Median
	60.0%	86,074
	70.0%	131,045
Fourth	Average	135,783
	75.0%	150,000
	80.0%	218,974
	90.0%	347,690
	95.0%	463,182
	97.5%	708,645
	99.0%	885,870
	Max	969,386

80%
90%
95%

Table 5

Incident Cost – 5 Years (2016–2020)

(N=222)

Quartiles		
First	Min	206
	1.0%	327
	2.5%	1,695
	5.0%	2,350
	10.0%	5,000
	20.0%	14,308
Second	25.0%	17,694
	30.0%	21,759
	40.0%	32,414
Third	50.0%	50,000 Median
	60.0%	64,336
	70.0%	96,785
Fourth	75.0%	107,834
	Average	119,887
	80.0%	135,900
	90.0%	277,059
	95.0%	492,642
	97.5%	721,250
	99.0%	993,571
	Max	2,546,712

80%
90%
95%

Table 6

Crisis Services Cost – 1 Year (2020)

(N=6)

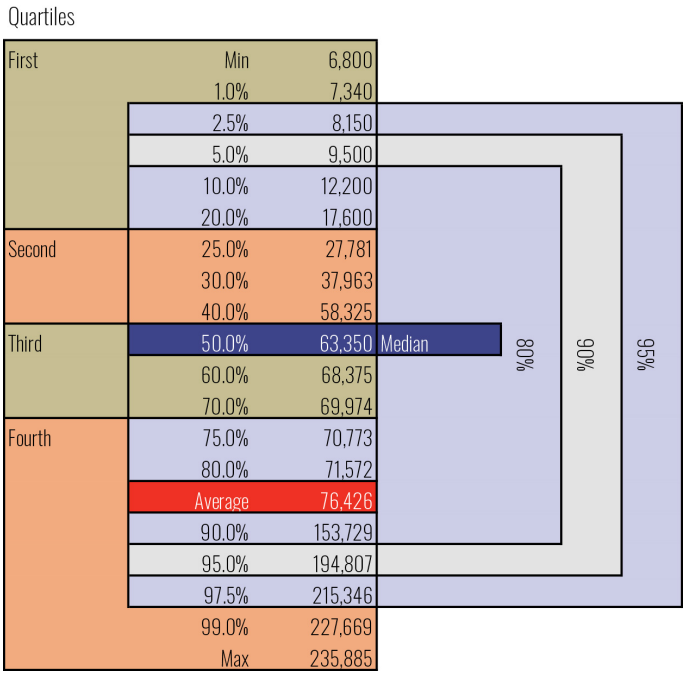

Table 7

Crisis Services Cost – 5 Years (2016–2020)

(N=80)

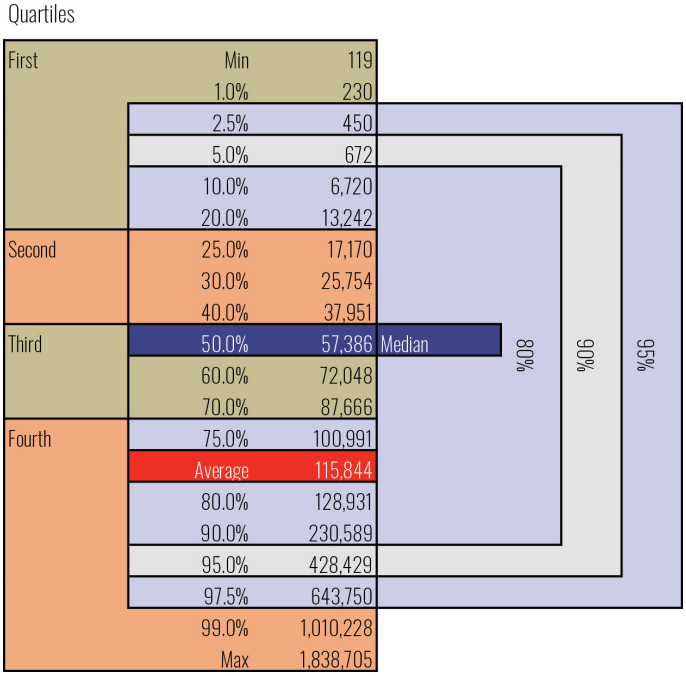

Table 8

Ransomware Cost – 1 Year (2020)

(N=18)

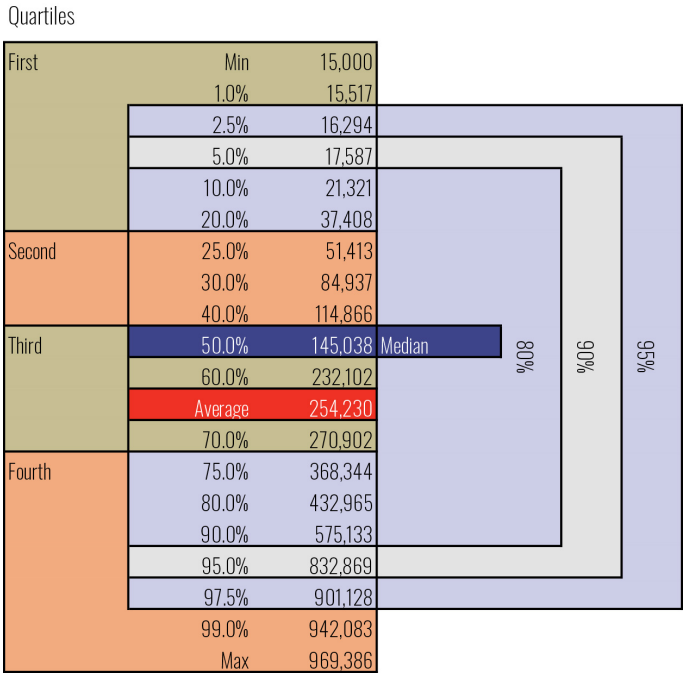

Table 9

Ransomware Cost – 5 Years (2016–2020)

(N=72)

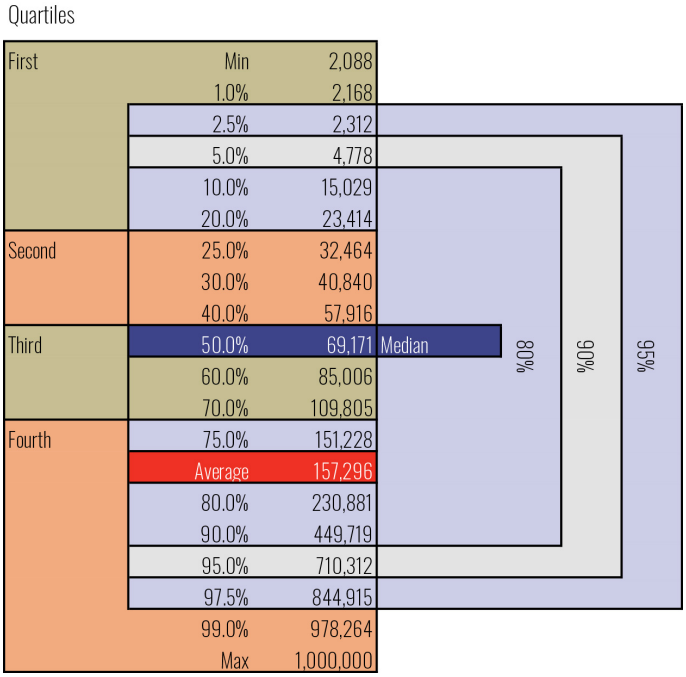

Table 10

Per-Record Cost – 5 Years (2016–2020)

80% of Data (Percentiles 10-90)

(N=31)

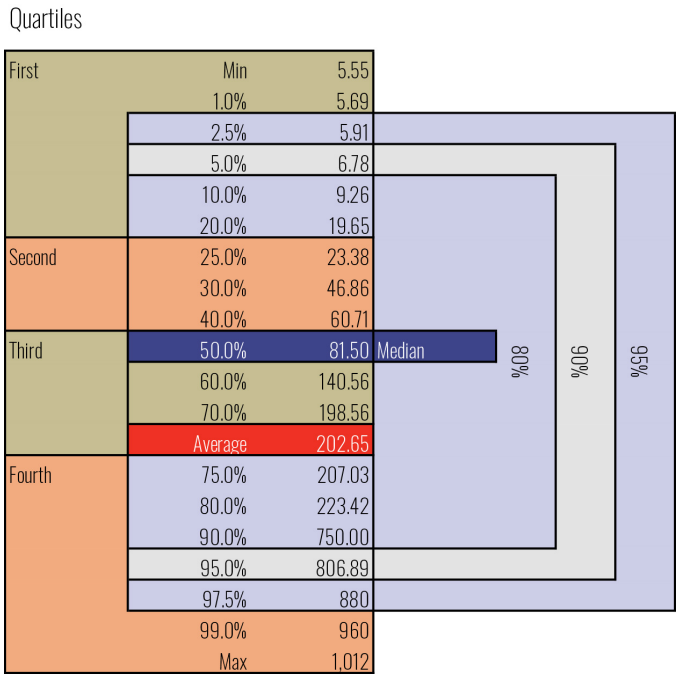

Table 11