NetDiligence®

CYBER CLAIMS STUDY

2025 INSIGHTS REPORT ON MANUFACTURING

CONSTANGY Brooks Smith & Prophete

experian.

RSM

SUREFIRE CYBER

Table of Contents

Introduction

Welcome to this NetDiligence® *Cyber Claims Study: 2025 Manufacturing Insights Report.*

The manufacturing sector in the United States is vast, encompassing enterprises ranging from garage-based boutiques to industrial giants with nearly $400B in annual revenue. Estimates for the number of organizations in the United States range from approximately 250,000 to over 600,000.

The sector has also ranked consistently in the top tier of sectors experiencing cyber loss. The recently published NetDiligence *2025 Cyber Claims Study* showed that manufacturing claims accounted for 8% of all claims and 13% of total incident cost at SMEs.

NetDiligence has responded with this *Insights Report*. Analyzing a subset of over 800 manufacturing claims, selected from the 10,500 claims in the 2025 NetDiligence dataset (2020-2024), we examined the effect of cyber claims on the manufacturing industry.

Our cyber claims dataset reflects the size variance found in the industry. Claims were gathered from organizations ranging from <$40K in annual revenues to >$130B. Total incident costs range from <$1,500 to more than $100M.

Because there are so few claims from large companies, the primary focus of this report is the claims experience at SMEs.

Key Findings

Cybersecurity threat actors have ramped up their attacks on manufacturing during the past five years. Extortion, theft of money, and theft of data are their goals. Ransomware, business email compromise (BEC), and wire transfer fraud are their primary means.

Some key numbers related to manufacturing claims and losses over the 5-year window:

- The average incident cost at SMEs (annual revenue <$2B) was $395K. The greatest incident cost was >$100M.
- The average incident cost at large companies (annual revenue≥$2B) was $8.5M. The greatest incident cost was over $50M.
- The average business interruption cost at SMEs was $2.5M, with a corresponding incident cost = $3M. The greatest BI cost was $100M, with a corresponding incident cost = $108M.
- The average business interruption cost at large companies was $12.2M, with a corresponding incident cost = $19.5M. The greatest BI cost was $46M, with a corresponding incident cost = $55M.
- At SMEs, ransomware and business email compromise accounted for 77% of claims and 94% of total incident costs.
- The average ransomware incident cost at SMEs was $409K. The maximum was over $100M.
- When comparing incidents at SMEs that reported both a ransom demand and a ransom paid, the average ransom demand was $4.9M and the average ransom paid was $936K, resulting in a savings of approximately 80%.
- The average BEC incident cost at SMEs was $70K.

Methodology

For a complete discussion of the methodology used to analyze the data and prepare *2025 Manufactuting Insights Report*, please see the Methodology section at the end of the *2025 Cyber Claims Report*.

Determining Total Incident Cost

Total incident cost is the best estimate of the total cost of an incident. It includes:

- SIR
- Ransoms
- Wire fraud amounts
- Crisis services costs
- All types of legal costs including litigation expense, settlements, and regulatory fines
- PCI-related costs
- Business interruption losses
- Recovery expense
- Any other costs that might have been provided for a claim, even if excluded from coverage by policy provisions

THANK YOU TO OUR SPONSORS

CONSTANGY
Brooks Smith & Prophete

experian.

RSM

SUREFIRE
CYBER

Demographic Information

Of the total claims in the five-year data set, manufacturing represents slightly less than 8%, making it third among sectors tracked in the study. A total of 820 claims from the manufacturing sector were reported.

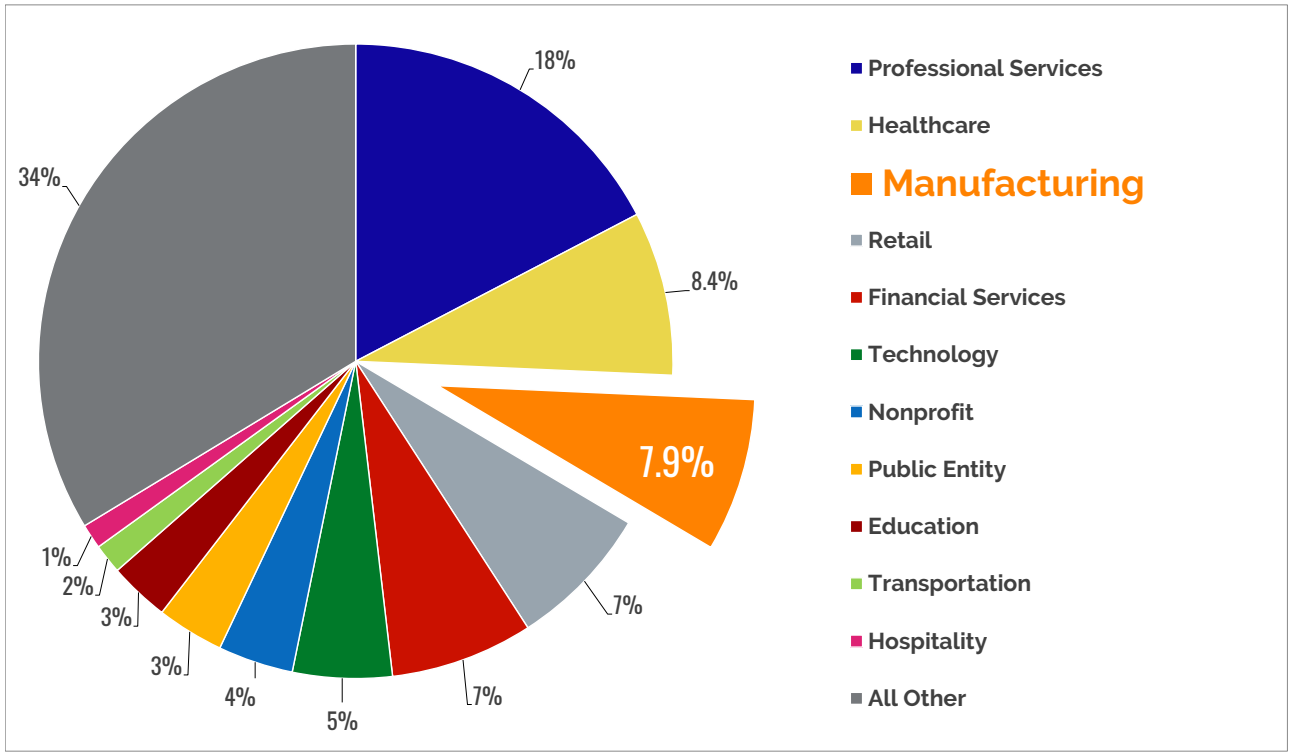

Figure 1

Figure 2 illustrates what percentage of these 820 claims were reported in each of the five years covered by the current dataset. We may expect the percentage of claims for 2024 to rise as we continue to collect data over the next few cycles.

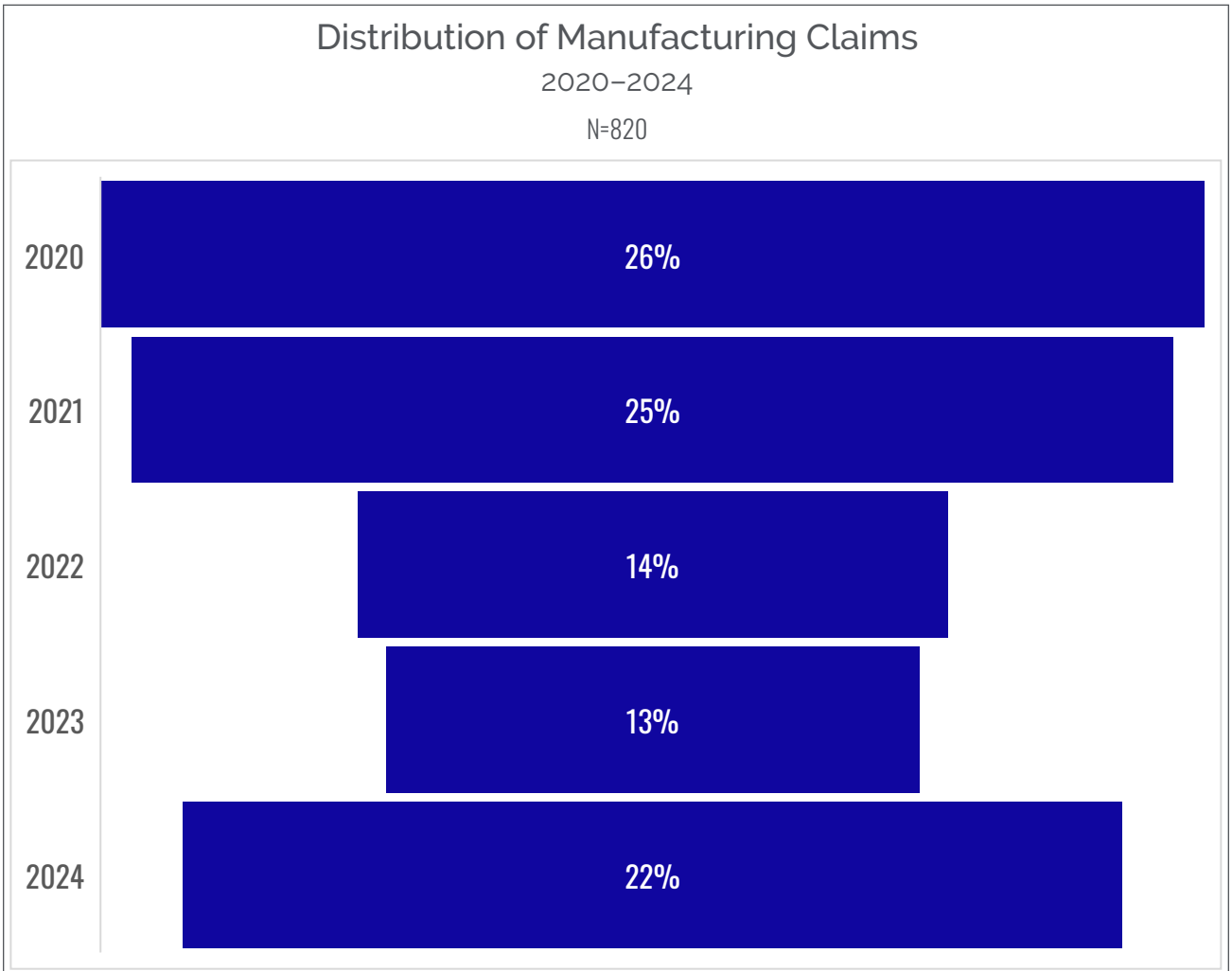

Figure 2

Incidents at SMEs accounted for 97% of these claims and incidents at large companies accounted for 3%. These proportions are close to those reported for all claims (N=10,400) in the annual report, 98% and 2%, respectively. (Figures 3 and 4)

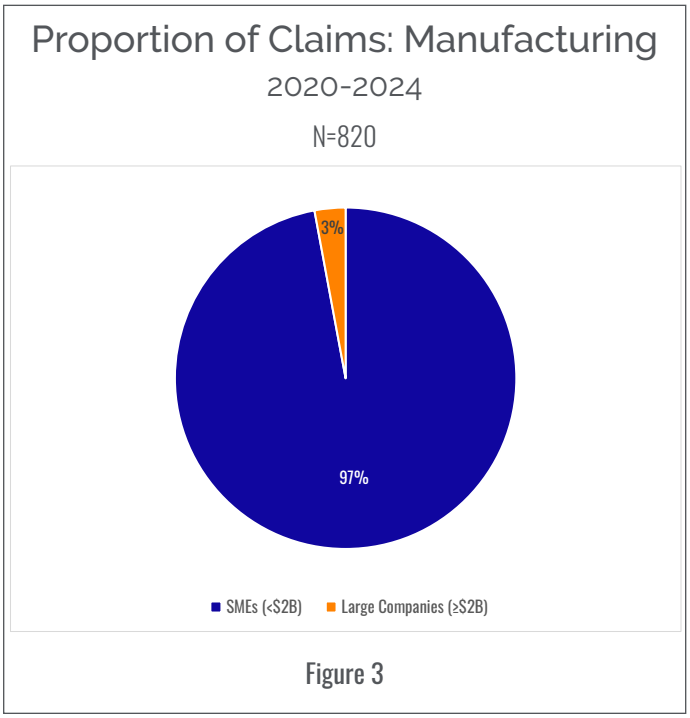

Figure 3

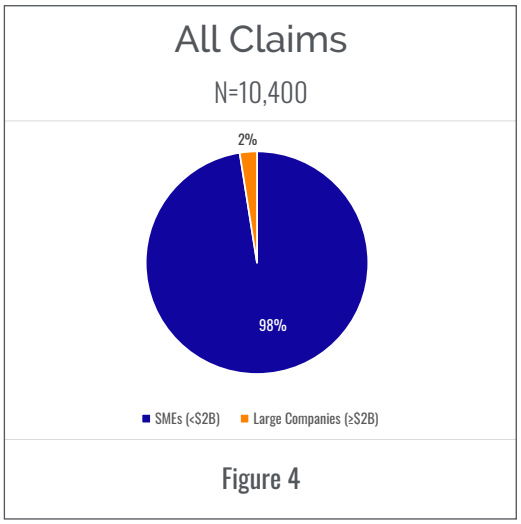

Figure 4

Claims at SMEs accounted for 61% of aggregate losses at SMEs and 39% at large companies, proportions that differ somewhat from those reported in the larger cyber claims report (49% and 51% respectively).

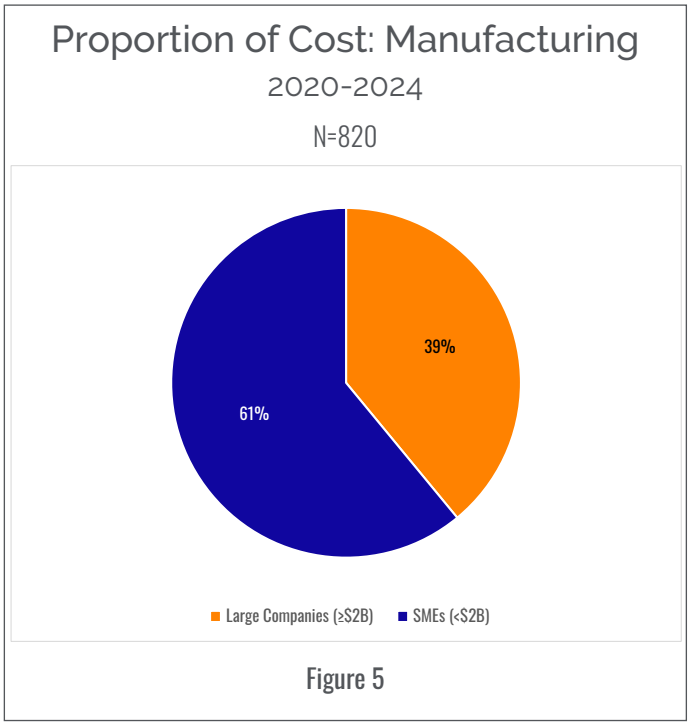

Figure 5

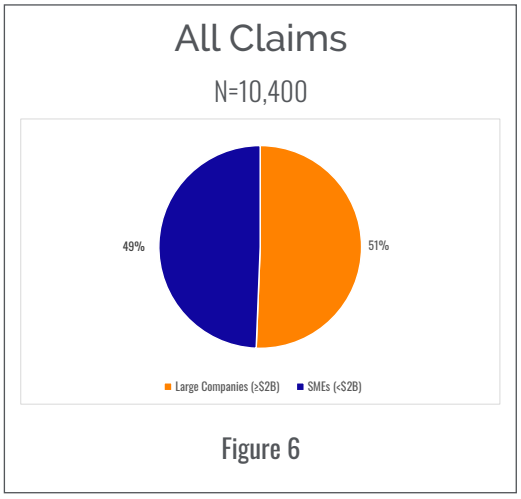

Figure 6

Total Incident Costs

Average payouts and total incident costs at SMEs were calculated from 773 cyber claims. Except for the average in 2022, which is heavily influenced by a single very large incident, the averages do not differ that much from the overall incident costs reported in the annual cyber claims report. The five-year averages are also skewed by a large event.

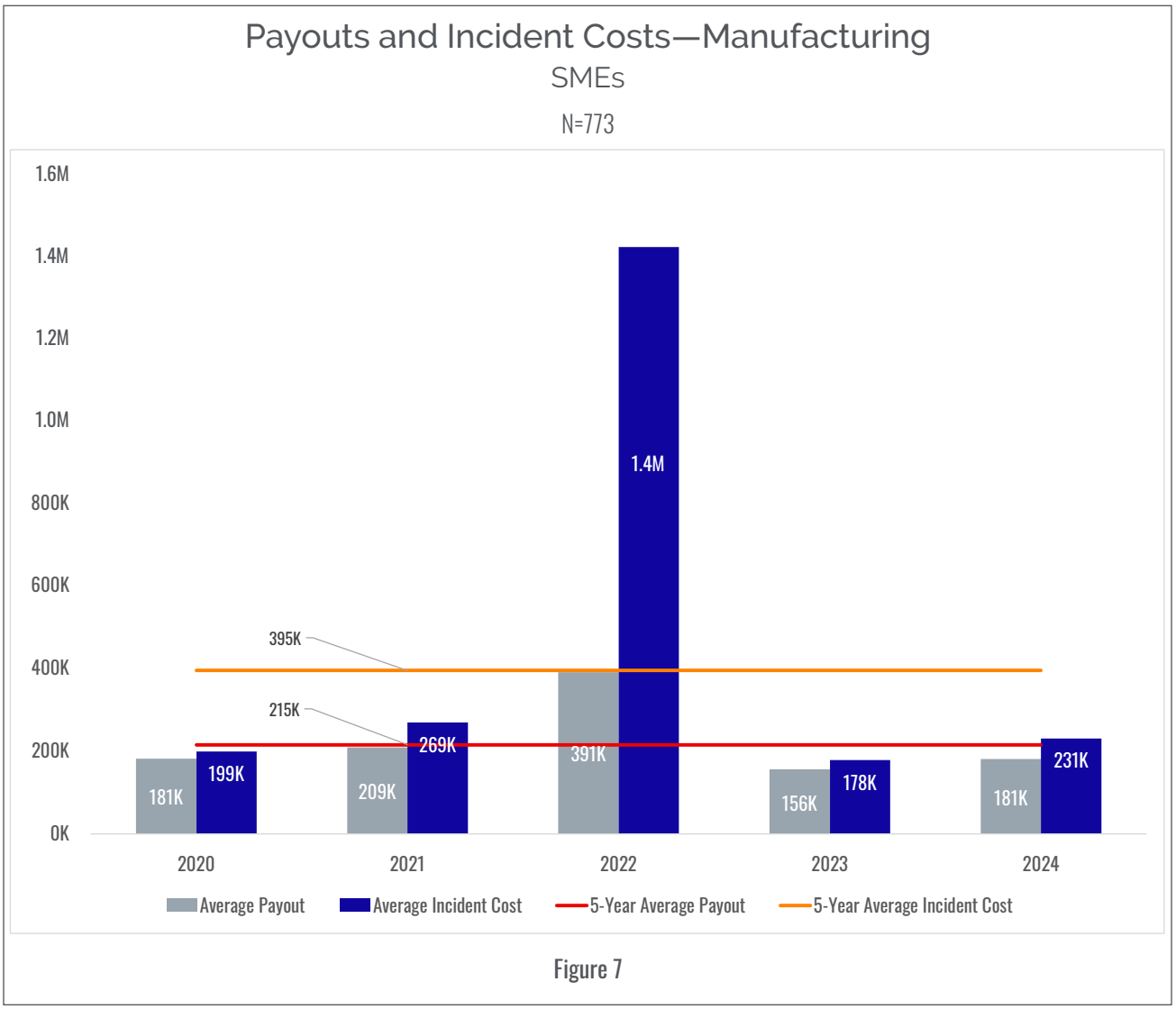

Figure 7

Except for 2022, the overall averages of total incident costs in the manufacturing sector were about the same as those of all other sectors. As mentioned above, the single large incident in 2022 is heavily skewing the five-year averages.

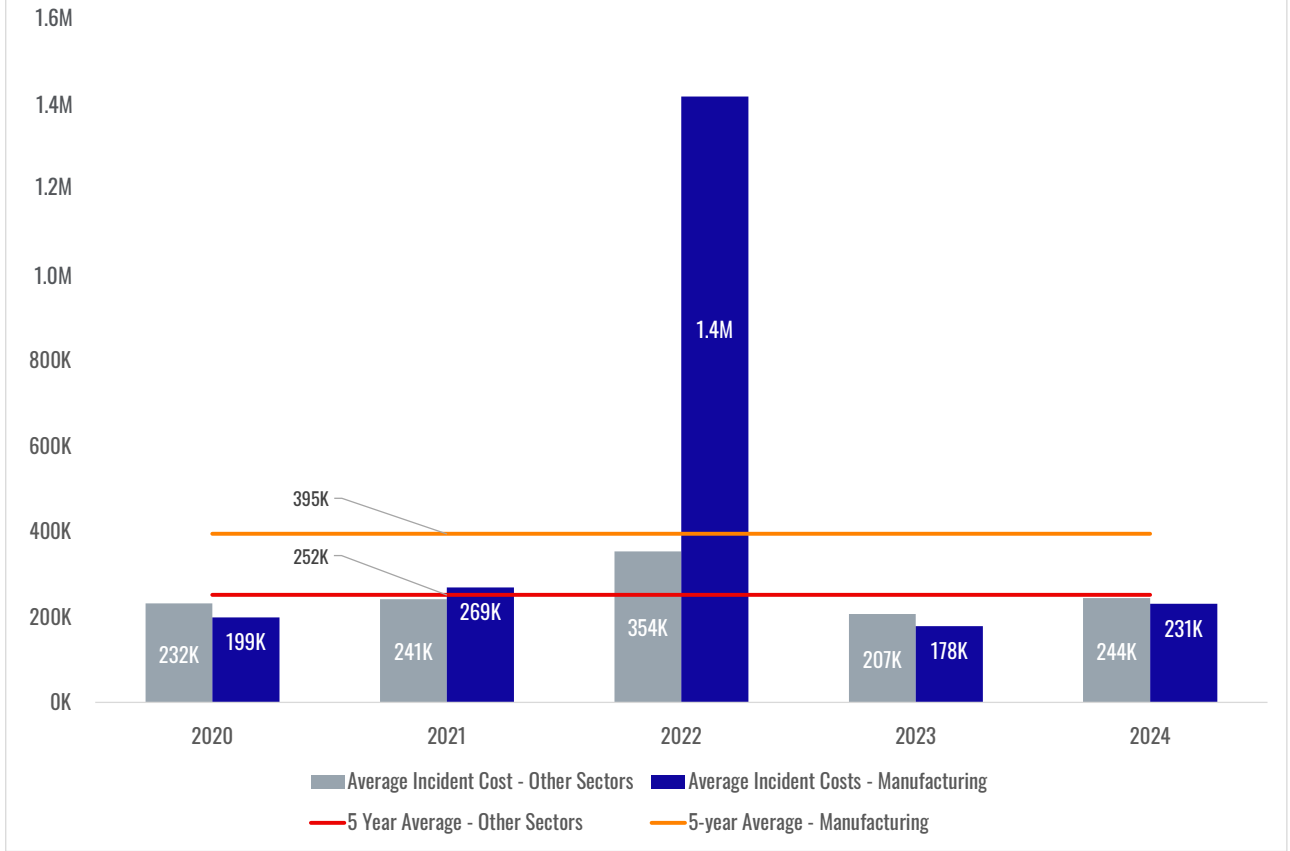

Figure 8

The five-year average incident cost at large companies was $8.5M, ranging from a low of $900K in 2022 to a high of $12.7M in 2020. There were only 23 large company incidents, so readers should bear this in mind when evaluating the numbers.

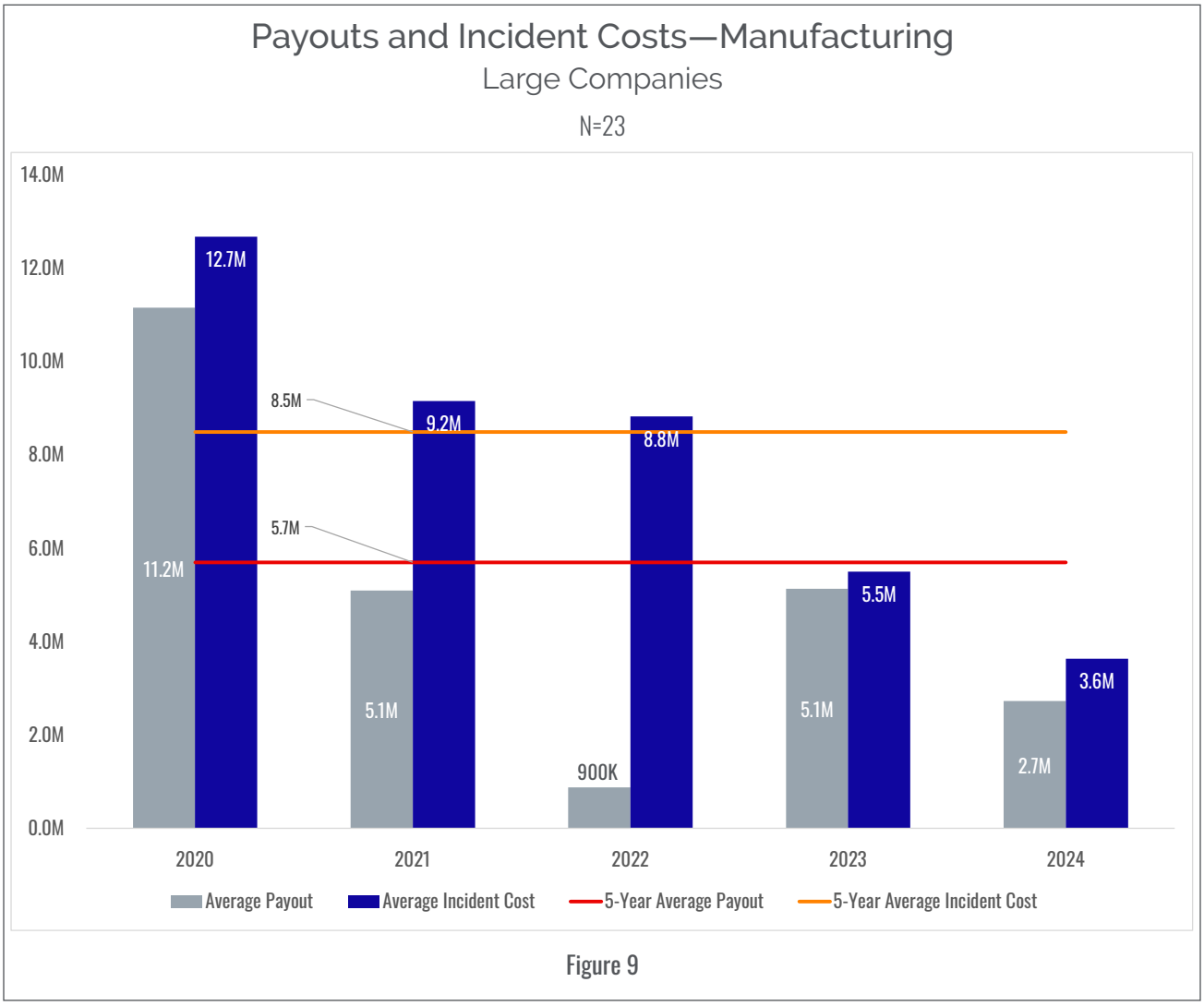

Figure 9

Crisis Services Costs

Total crisis services costs were reported for 76% of incidents at SMEs. The five-year average of the costs was $138K with a corresponding average incident cost = $441K. The large incident in 2022 did not report any amount for total crisis service so the five-year average was not skewed.

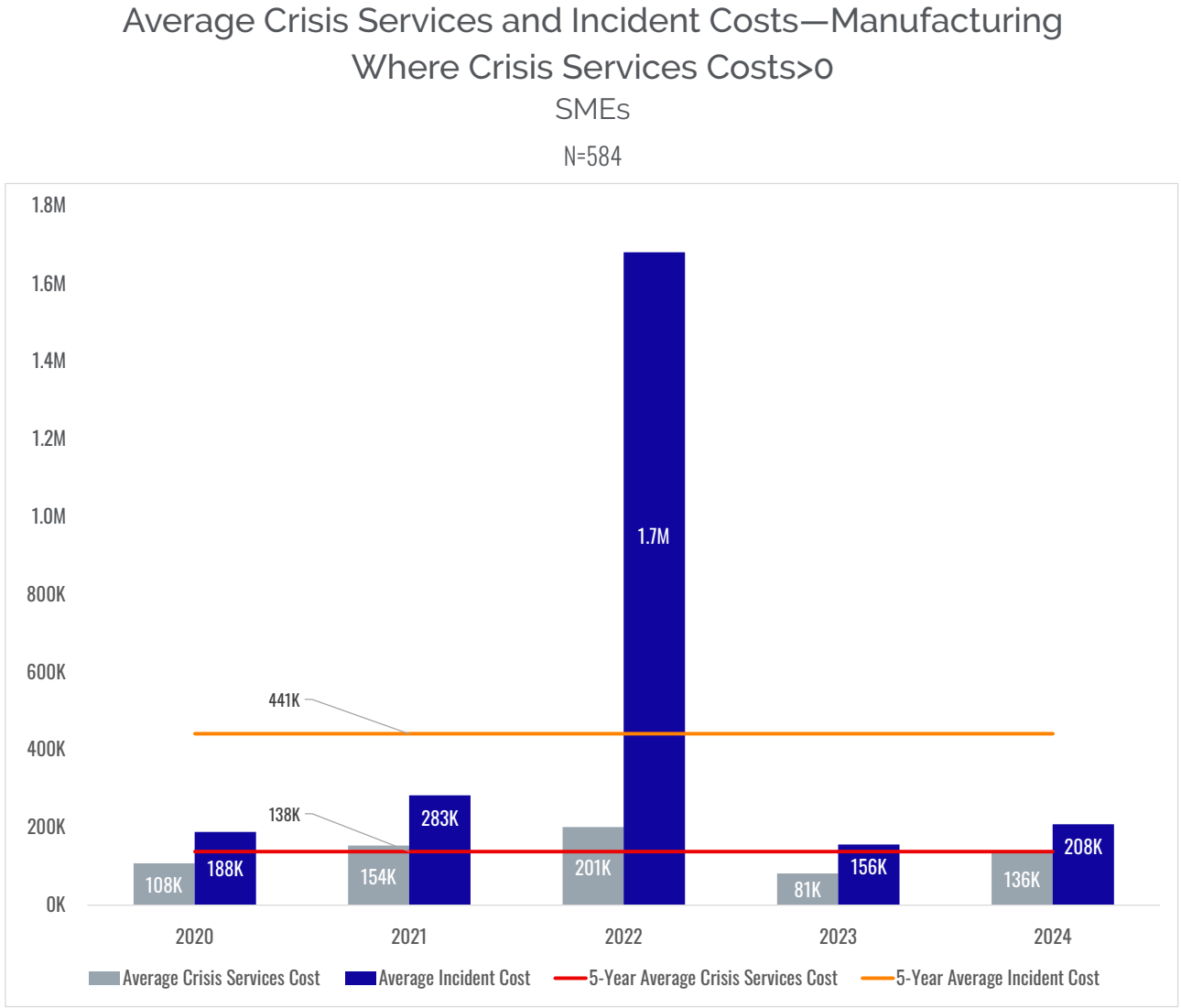

Figure 10

Overall total crisis services for five years accounted for 31% of total incident costs, ranging from a low of 12% to a high of 65%.

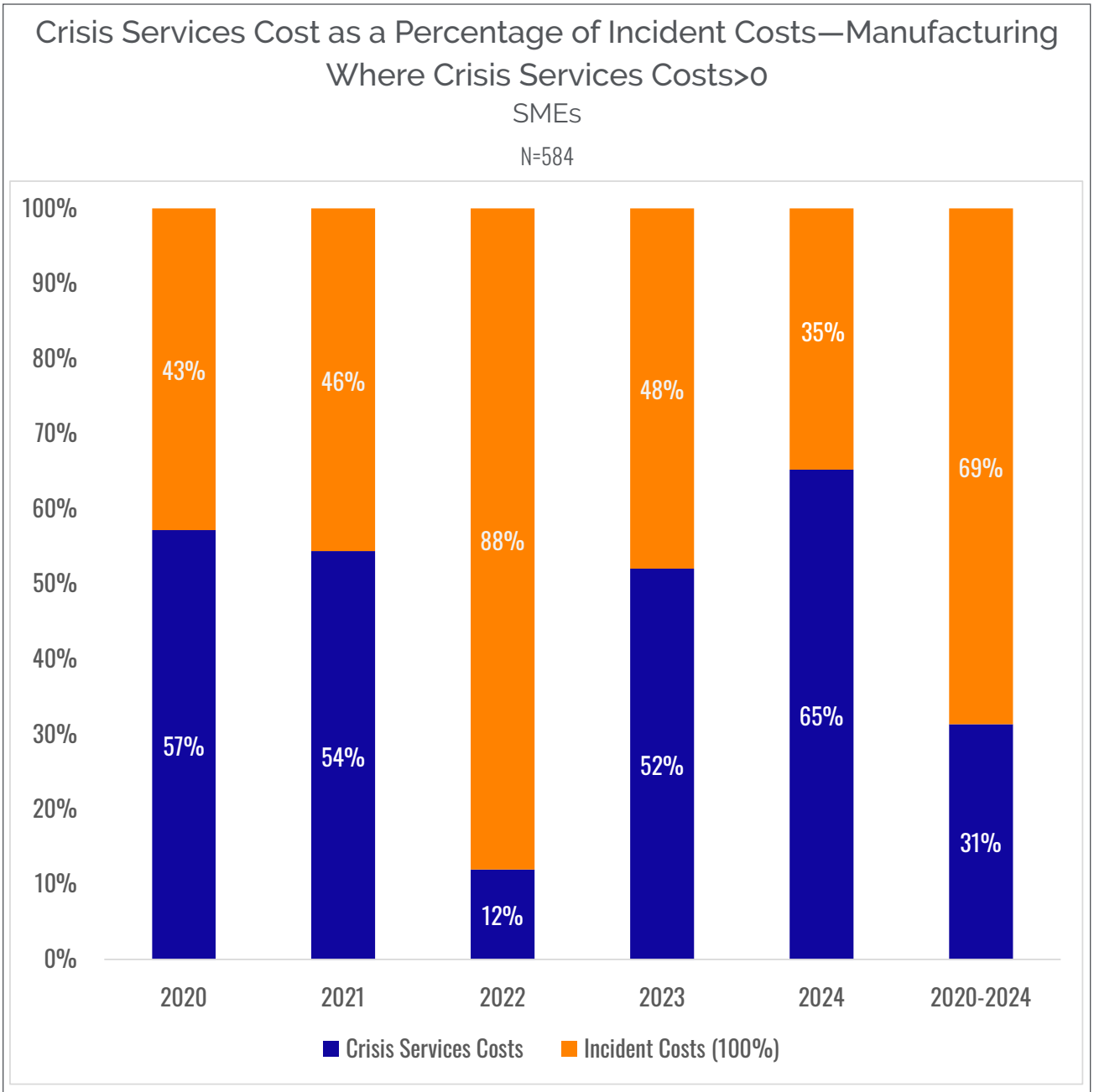

Figure 11

Table 1 below details the average costs for the components of crisis services.

Crisis Services Costs—Manufacturing
SMEs
2020–2024

Service	Minimum	Average	Maximum	Total
Forensics	0K	71K	5.0M	26.8M
Credit Monitoring	0K	2K	21K	60K
Notification	0K	7K	86K	593K
Legal Guidance	0K	22K	459K	9.0M
Other Crisis	0K	98K	1.1M	33.6M

Table 1

Business Interruption

51 claims from SMEs reported BI costs. The averages ranged from $264K to $10.5M, with corresponding total incident costs ranging from $429K to almost $12.5M. The numbers from 2022 were heavily influenced by a single event with BI and total incident costs ≥$100M.

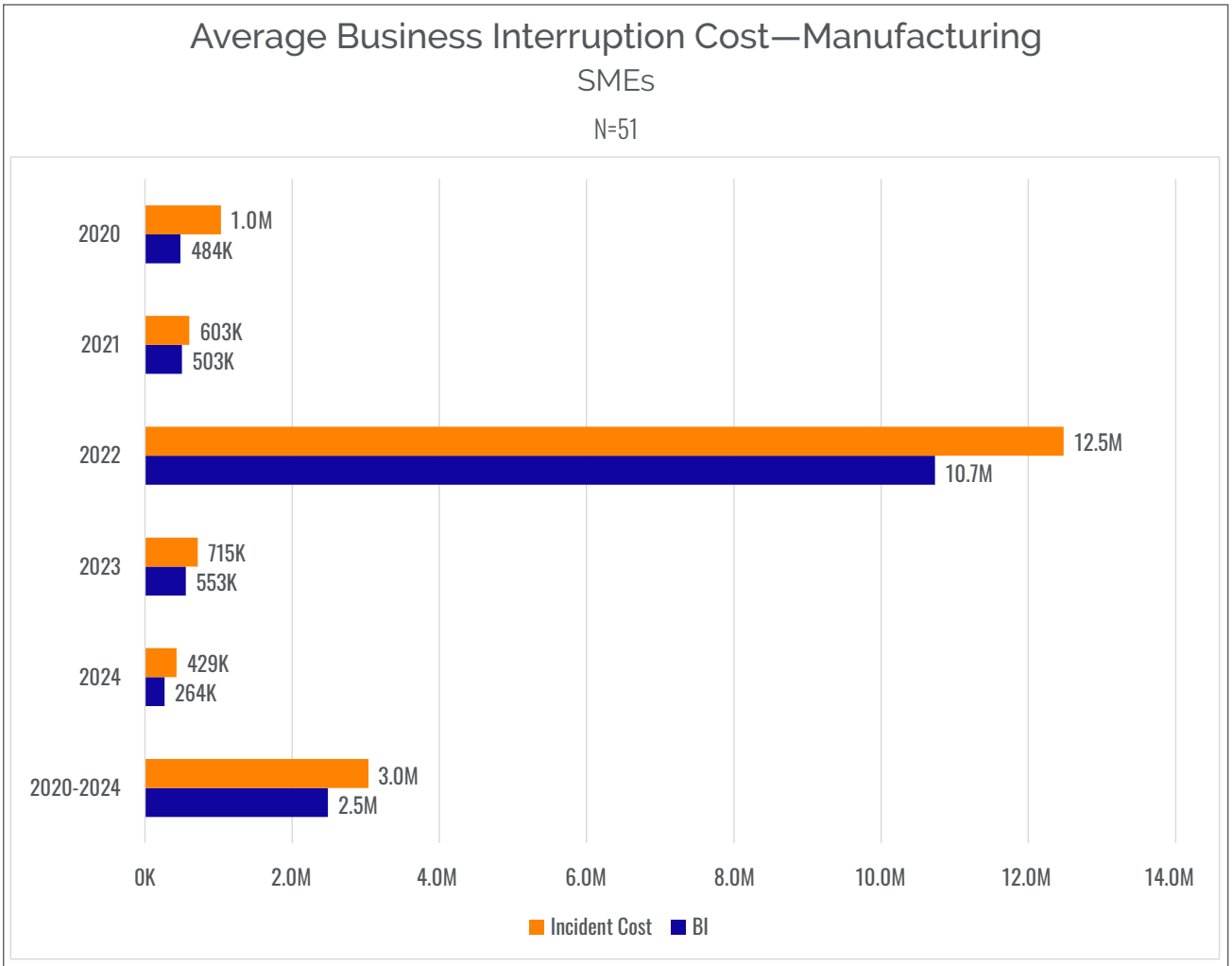

Figure 12

Causes of Loss at SMEs

Cause of loss was reported for 81% for claims analyzed. Ransomware and BEC were the primary causes of loss for incidents in the manufacturing sector, accounting for 77% of claims and 94% of total incident costs. Wire transfer fraud accounted for 3% of claims and all other causes of loss represented <1% each.

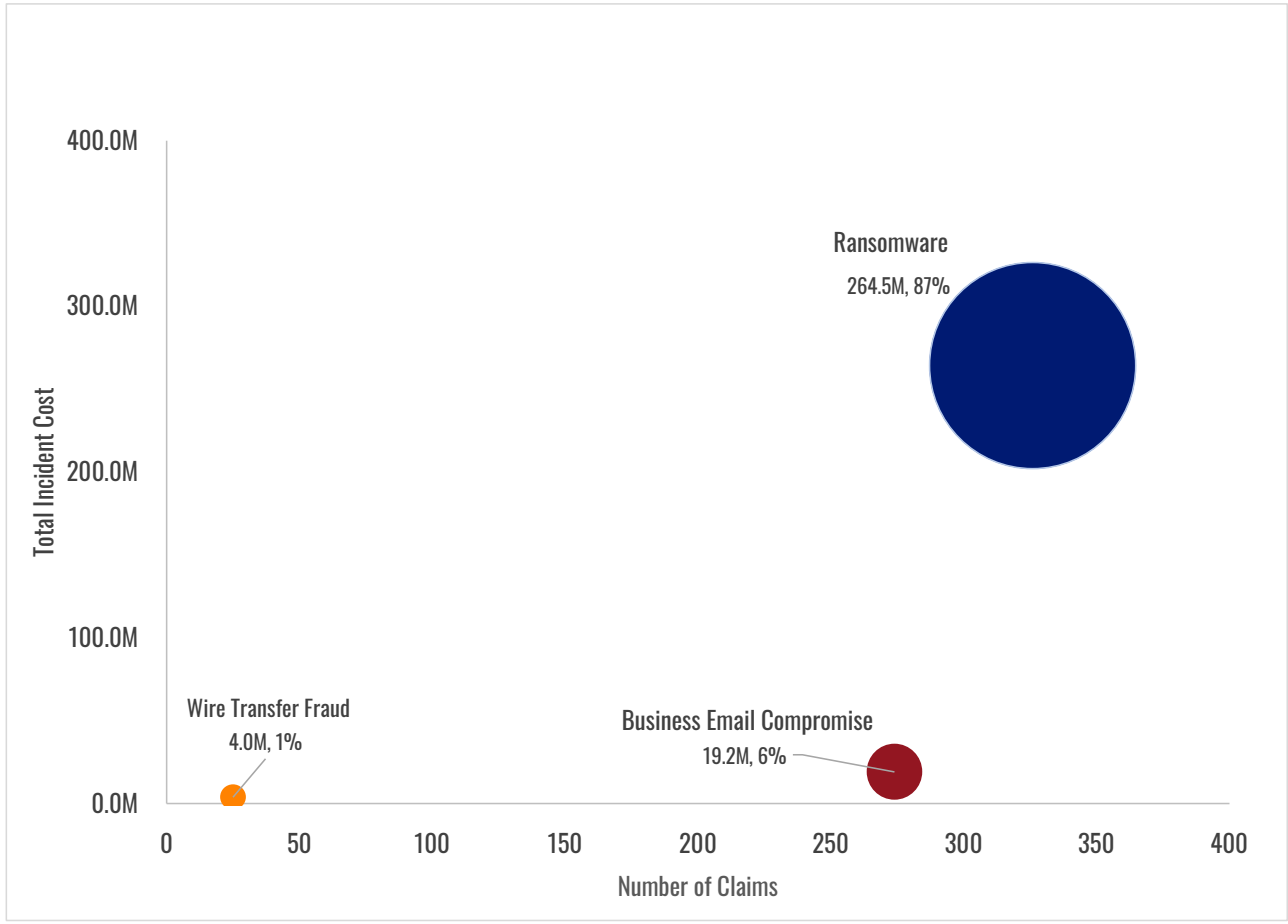

Figure 13

Ransomware

There were 326 ransomware claims reported for the five-year period. These claims represented 42% of all claims in the sector (cause of loss reported or not) and over 87% of aggregate incident costs. Average incident costs ranged from $345K to almost $3.5M. The skewing impact of the large incident in 2022 is once again evident in the graph below.

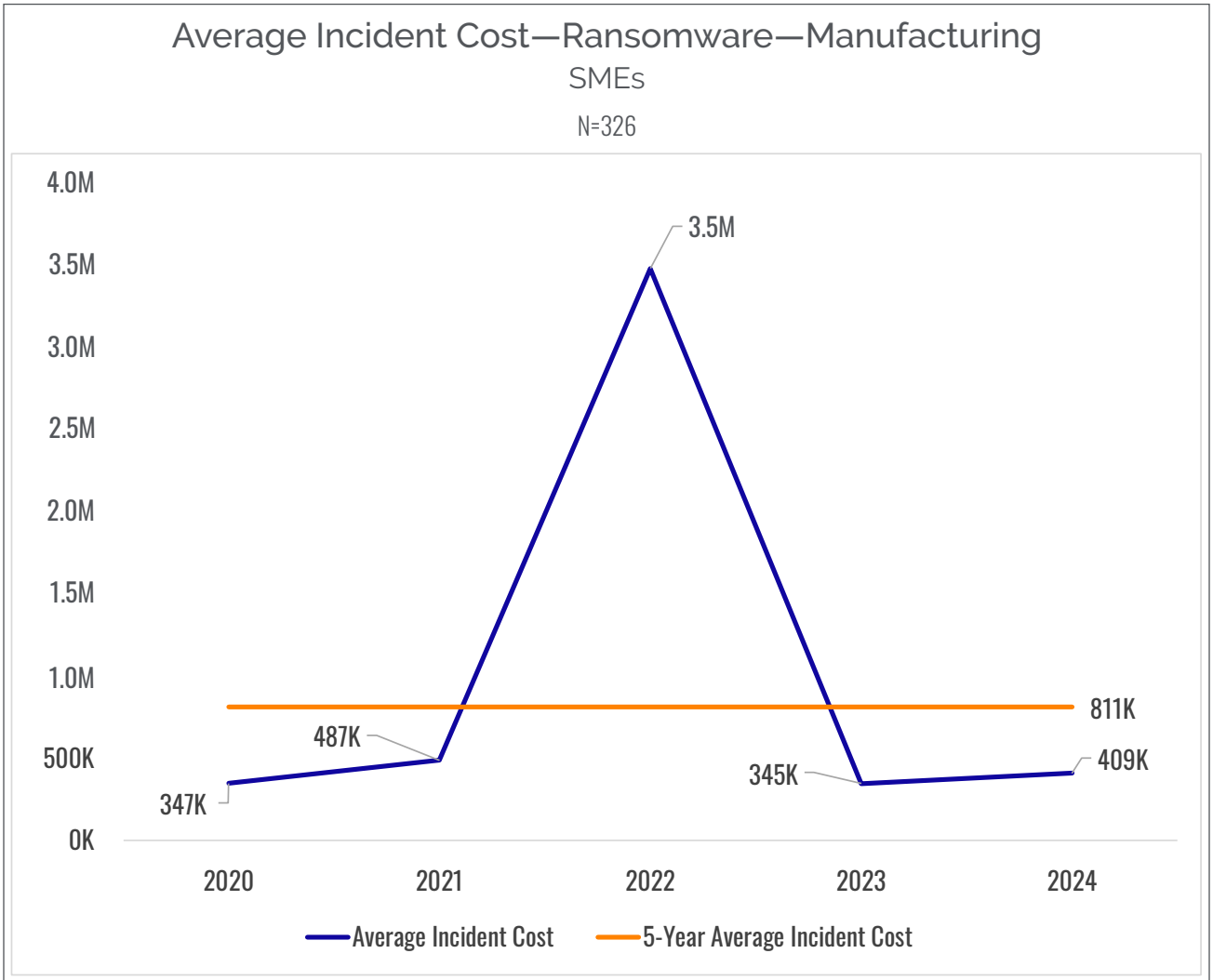

Figure 14

When comparing the incidents that reported both an initial ransom demand and a final ransom amount paid, the savings ranged from $400K (33%) to $12.3M (93%), with a five-year average savings of over 80%. These variances are consistent with findings from other NetDiligence reports, suggesting that negotiating with threat actors can yield substantial savings.

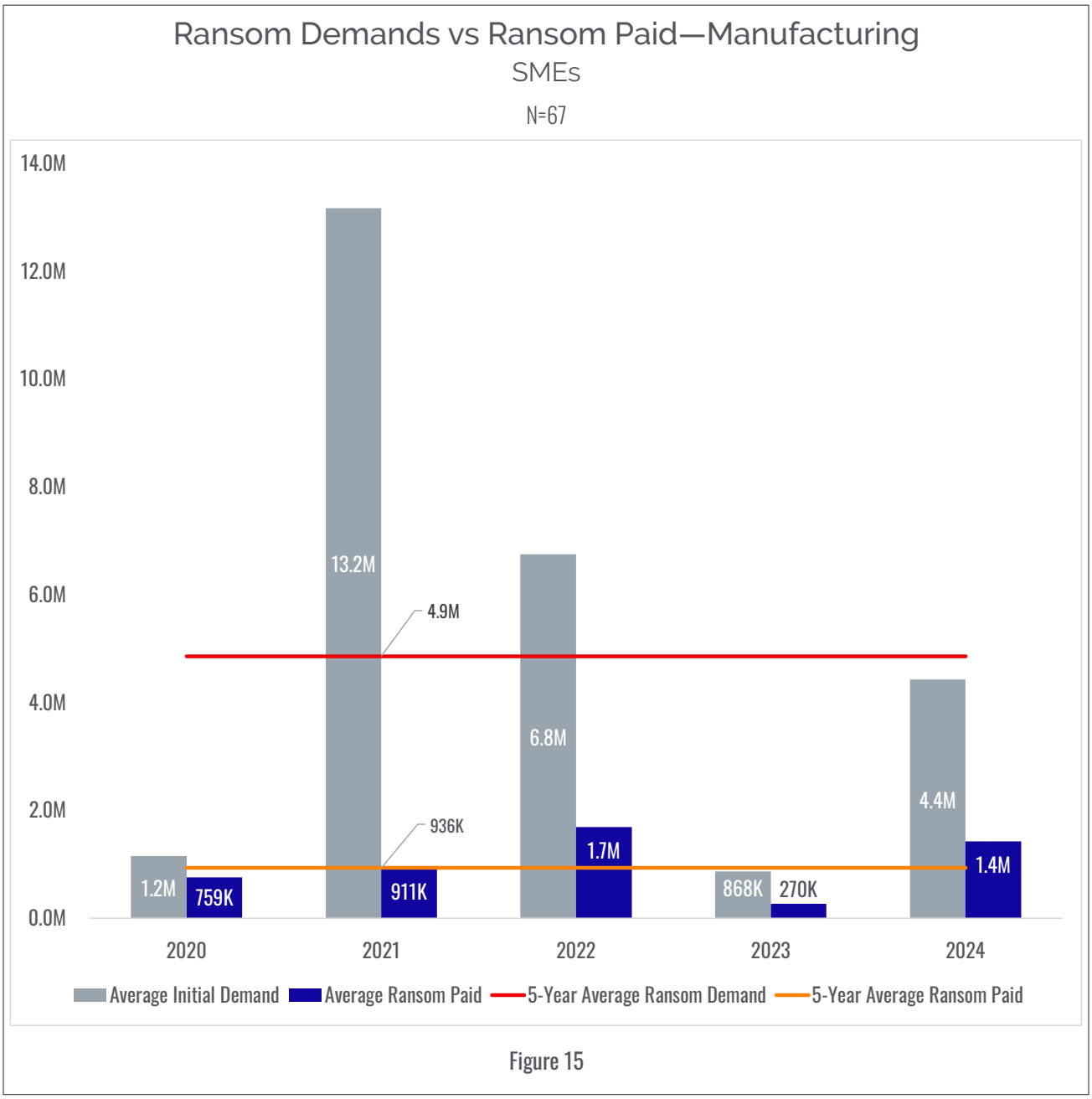

Figure 15

Business Email Compromise (BEC)

BEC claims accounted for 35% of all claims and 4% of aggregate incident costs. BEC incidents were generally low impact, with average costs ranging from $54K to 83K. The five-year average incident cost was $70K.

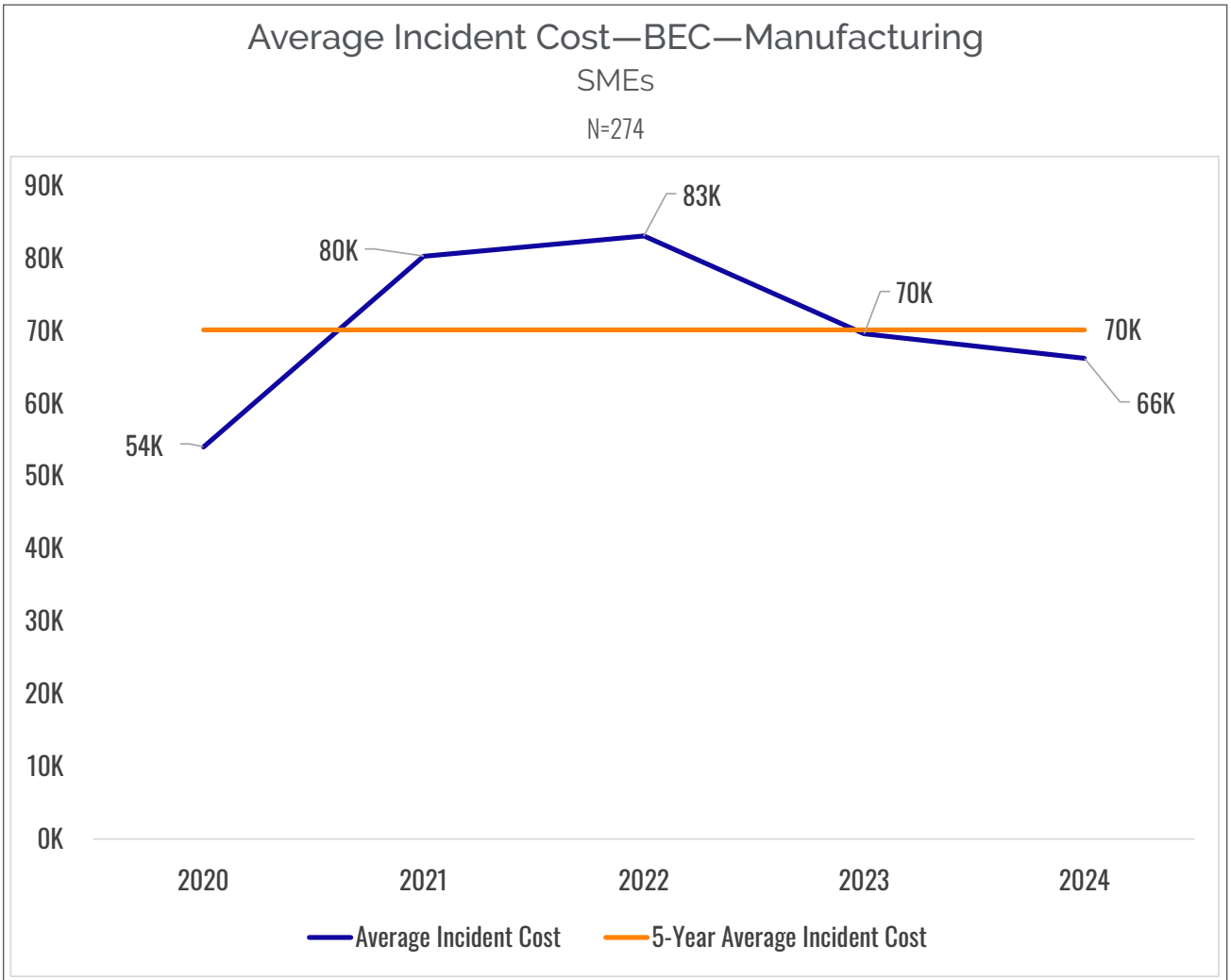

Figure 16

Wire Transfer Fraud

There were 54 wire transfer fraud claims in the dataset. The average incident costs ranged from $72K to $301K, with a five-year average of $156K. These averages are comparable to the average in other sectors as reported in the *2025 NetDiligence Cyber Claims Study* ($106K-$302K, five-year average=$160K).

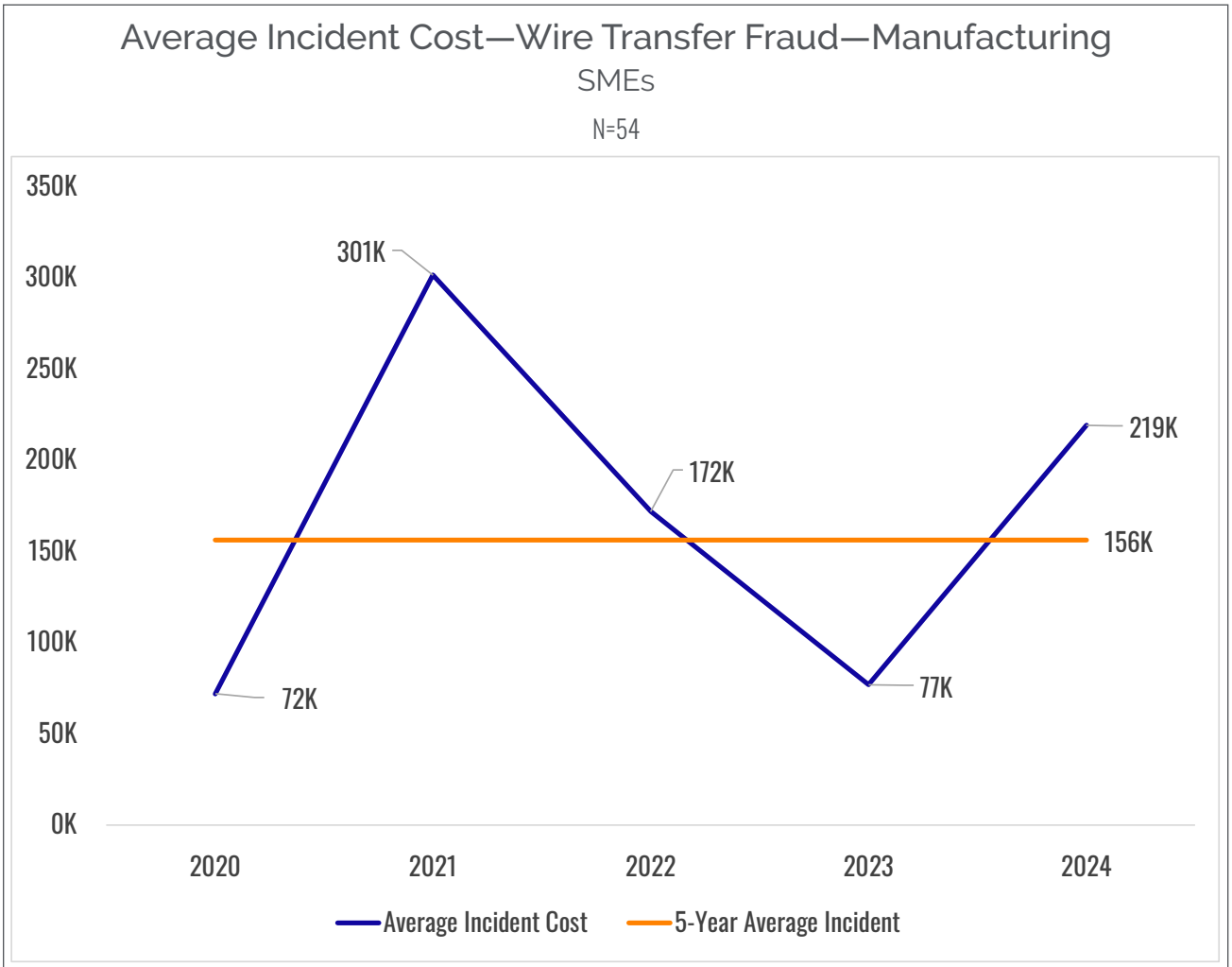

Figure 17

Incident Cost by Cause of Loss
Manufacturing—SMEs
2020-2024

Cause of Loss	Claims	Minimum	Average	Maximum	Total	% of Total	Rank by Claims	Rank by Cost
Business Email Compromise	274	6K	70K	1.3M	19.2M	6.3%	2	9
Cyber Event—Unspecified	6	12K	75K	209K	450K	0.1%	8	8
Hacker	20	4K	58K	309K	1.2M	0.4%	6	10
Lost/Stolen Laptop/Device	1	27K	27K	27K	27K	0.0%	13	14
Malware/Virus	21	11K	128K	847K	2.7M	0.9%	5	5
Phishing	5	13K	30K	60K	149K	0.0%	9	12
Ransomware	326	7K	811K	108.0M	264.5M	86.7%	1	1
Rogue Employee	3	24K	33K	39K	100K	0.0%	11	11
Staff Mistake	5	10K	255K	1.1M	1.3M	0.4%	9	2
System Glitch	1	93K	93K	93K	93K	0.0%	13	6
Theft of Hardware	3	5K	27K	52K	82K	0.0%	11	13
Theft of Money	10	1K	87K	200K	875K	0.3%	7	7
Wire Transfer Fraud	25	6K	160K	1.3M	4.0M	1.3%	4	3
Other	73	1K	144K	1.4M	10.5M	3.4%	3	4

Table 2

Average Crisis Services Costs by Cause of Loss
Manufacturing—SMEs
2020-2024

Cause of Loss	Forensics	Monitoring	Notification	Legal Guidance	Other	Total Crisis Costs	Rank by Total Crisis Cost
Business Email Compromise	14K	0K	9K	11K	53K	49K	6
Cyber Event—Unspecified	49K	0K	3K	5K	0K	54K	5
Hacker	34K	0K	2K	11K	49K	33K	9
Lost/Stolen Laptop/Device	0K	0K	2K	14K	0K	17K	13
Malware/Virus	19K	0K	6K	7K	281K	67K	3
Phishing	11K	0K	0K	3K	0K	14K	14
Ransomware	101K	3K	7K	31K	145K	245K	1
Rogue Employee	16K	0K	0K	3K	0K	18K	12
Staff Mistake	8K	0K	0K	2K	0K	66K	4
System Glitch	59K	0K	0K	9K	0K	68K	2
Theft of Hardware	2K	0K	0K	6K	0K	8K	15
Theft of Money	59K	0K	0K	7K	26K	26K	10
Wire Transfer Fraud	18K	0K	0K	7K	44K	26K	11
Other	18K	0K	7K	11K	44K	34K	7

Table 3

Conclusion

We hope that you have found the analysis to be helpful.

If you are not a current contributor to the annual *NetDiligence Cyber Claims Study*, please consider participating in 2026. We will begin collecting data in January 2026 and expect to publish the report in Fall 2026.

To download the 2025 *NetDiligence Cyber Claims Study Report* as well as other Insight reports, please visit the NetDiligence website at www.netdiligence.com.

Our Sponsors

About Constangy, Brooks, Smith & Prophete LLP

The Constangy Cyber Team is composed of over 85 members, including nearly 60 attorneys, offering a full suite of cybersecurity and data privacy services. These include compliance advisory (proactive services), incident response (over 3,000 incidents annually), and litigation (defending class actions in over 30 states). In 2025, the team was recognized by Intelligent Insurer as "Law Firm of the Year."

About RSM US LLP

RSM is the leading provider of professional services to the middle market. The clients we serve are the engine of global commerce and economic growth, and we are focused on developing leading professionals and services to meet their evolving needs in today's ever-changing business landscape. For more information, visit rsmus.com, like us on Facebook, follow us on Twitter and/or connect with us on LinkedIn.

About Experian

When every minute counts, count on Experian Data Breach Resolution for the partnership, solutions, and performance to create the best possible outcome. With 20+ years' experience, we've managed some of the largest and highest-profile breaches in history. Our turnkey offerings include Experian Reserved Response™, data breach response, crisis response management, and identity protection. Discover more at http://www.experian.com/databreach or email databreachinfo@experian.com.

About Surefire Cyber

Surefire Cyber is redefining the incident response model by delivering a swifter, stronger response to cyber incidents such as ransomware, email compromise, malware, data theft, and other threats. Our client-centric approach reduces stress and provides clients the confidence needed to prepare, respond, and recover from cyber incidents—and fortify their cyber resilience after an event.

About NetDiligence®

NetDiligence® is a trusted leader in Cyber Risk Readiness & Response—serving the cyber insurance ecosystem for over two decades. Since 2001, we've helped insurers, brokers, and policyholders reduce the impact of cyber incidents with proven tools, services, and education rooted in real-world claims data.

Our mission is twofold: **proactively support cyber resilience** and **empower swift, effective response** when incidents occur. From benchmark research and interactive tools to policyholder portals and mobile apps, our solutions help make cyber risk more manageable—and insurable.

Breach Response, Ready When You Need It

Breach Plan Connect® is a dynamic, cloud-hosted incident response solution designed to keep organizations operational in the face of a cyber crisis. Pre-loaded with expert-vetted best practices and fully customizable, it helps teams respond decisively to ransomware, BEC, and more.

Key features include guided plan-building, integrated breach response playbooks, and a **mobile app** for anytime-anywhere access—even when systems are compromised. It's trusted by insurers, IT leaders, and legal teams to turn chaos into clarity during critical moments.

A Smarter Portal for Cyber Policyholders

The eRiskHub® is more than just a policyholder resource—it's an interactive cyber risk management platform that insurers use to **educate, empower, and differentiate** their cyber product. Fully white-labeled and customizable, it delivers threat intelligence, risk tools, breach response vendors, and much more.

With over 70,000 users globally, eRiskHub helps insureds build readiness—and insurers control loss ratios.

Cyber Risk Assessments Beyond the Checklist

Our QuietAudit® suite of assessments helps organizations truly understand their cyber risk exposure—not just check a compliance box. We combine deep-dive consultant-led reviews with automated self-assessments, offering actionable insights for organizations of all sizes and industries.

Assessments are tailored to support underwriting, vendor due diligence, and litigation defense, and include add-on options like network vulnerability scans and tabletop exercises.

Where the Industry Connects

Our Cyber Risk Summits are the cyber insurance industry's premier networking events—bringing together underwriters, claims professionals, breach response experts, and risk managers from around the world.

Programs are expertly curated to address both emerging threats and practical challenges faced by cyber insurers and their clients. In 2026, join us in Miami Beach, Toronto, San Diego, and Philadelphia for next-level insights and connections that move the industry forward.

Contact Us

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

NetDiligence®