NetDiligence®

Annual Cyber Claims Study

2025 Report

Insights & Findings

NetDiligence®

NetDiligence® Cyber Claims Study

New Claims Submitted
(in 2025)

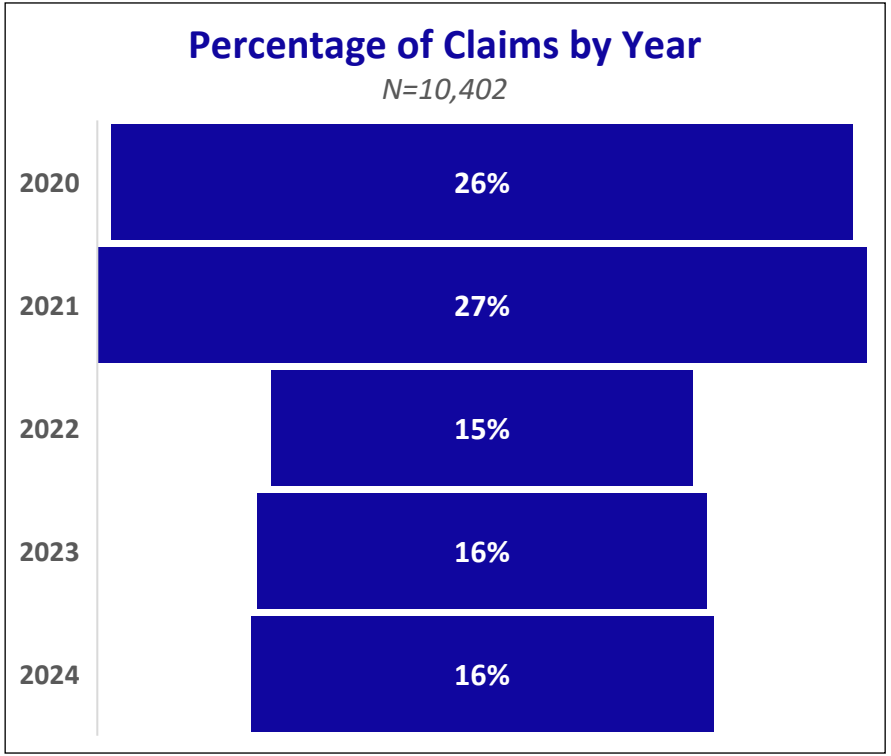
4,108

Claims in 2025 Dataset
(2020-2024)

10,402

Fun Fact:

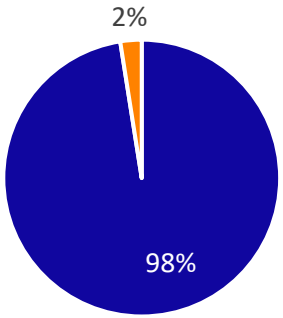
NetDiligence has been publishing the annual cyber claims study for 15 years and counting!



NetDiligence®

NetDiligence® Cyber Claims Study

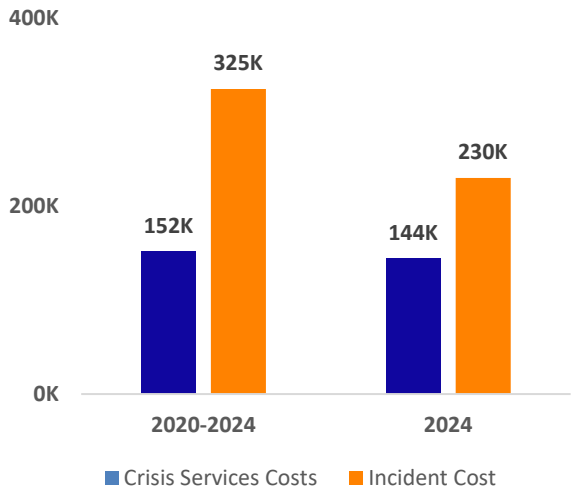
Proportion of Claims
(2020-2024)
N=10,402



Average Revenue Size	
SME	$108M
Large Company	$12.5B

SMEs

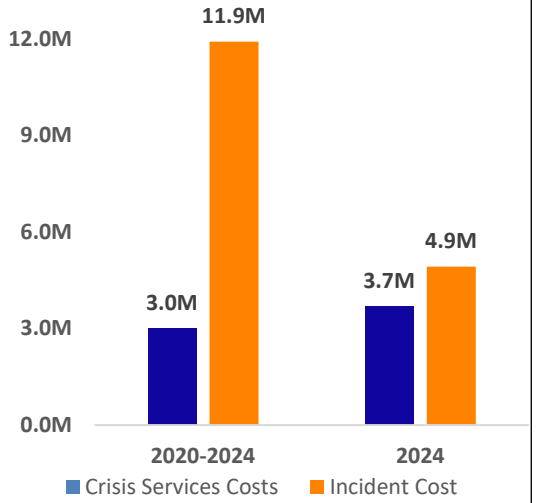
Average Costs
Crisis Services Costs >0
N=4,712



66 of 8,936 (0.7%) claims were >= $5M

Large Companies

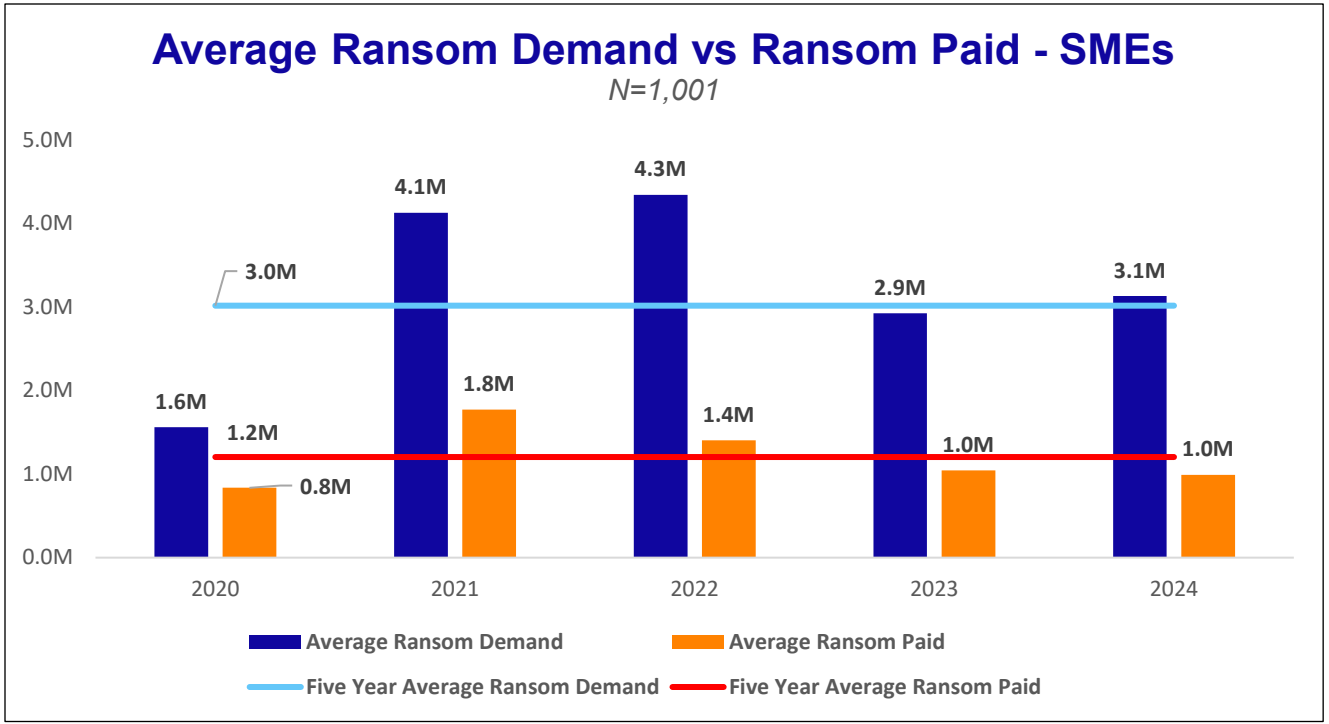
Average Costs
Crisis Services Costs >0
N=115



56 of 235 (24%) claims were >= $5M

NetDiligence®

NetDiligence® Cyber Claims Study



NetDiligence®

NetDiligence® Ransomware Advisory Board

—EVOLVING TRENDS AND COMMUNITY OBSERVATIONS—

The **Ransomware Advisory Board (RAB)** meets quarterly. This group and is comprised of prominent forensics vendors and law enforcement partners. **Recent trends reported from our Q1 2026 meeting are shown below.**

1. Weak MFA Is Creating a False Sense of Security

"MFA enabled" doesn't automatically mean accounts are secure. Attackers routinely bypass weak implementations—especially when SMS, email codes, or legacy authentication methods remain active. If phishing-resistant MFA isn't enforced and weaker backup options aren't removed, attackers will exploit the easiest path.

Key Takeaway: Strong MFA must be paired with strict session controls and secure account recovery processes to be effective.

2. Attackers Disable Security Tools and Persist After Resets

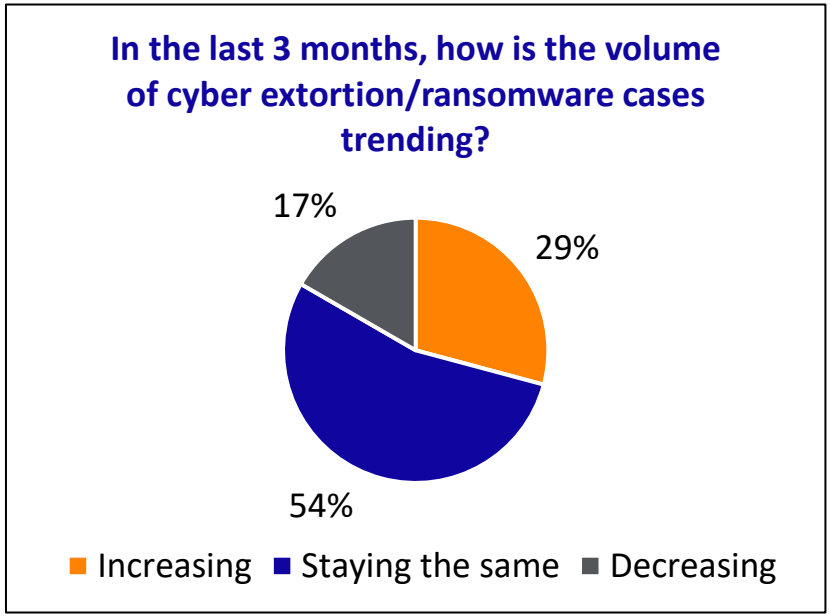
Threat actors are increasingly disabling EDR tools early in an incident using widely available techniques. Even after passwords are reset, stolen session tokens or API keys can keep attackers logged in if sessions aren't revoked.

Key Takeaway: Without full containment steps—including credential rotation and session invalidation—organizations risk prolonged attacker access.

3. Help Desk Exploitation and Response Delays Increase Impact

Help desks are a primary social engineering target, with attackers impersonating employees to reset passwords or enroll new MFA devices. At the same time, delayed escalation to professional responders gives attackers more time to expand access.

Key Takeaway: Rapid session revocation, SaaS containment, and clear response activation processes are critical to limiting damage.



NetDiligence®

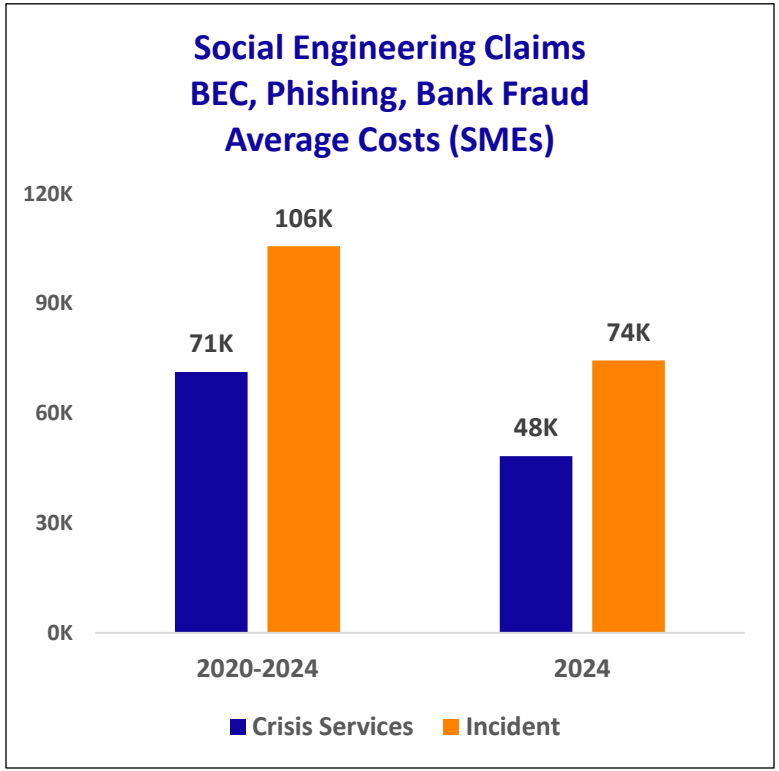
NetDiligence® Cyber Claims Study

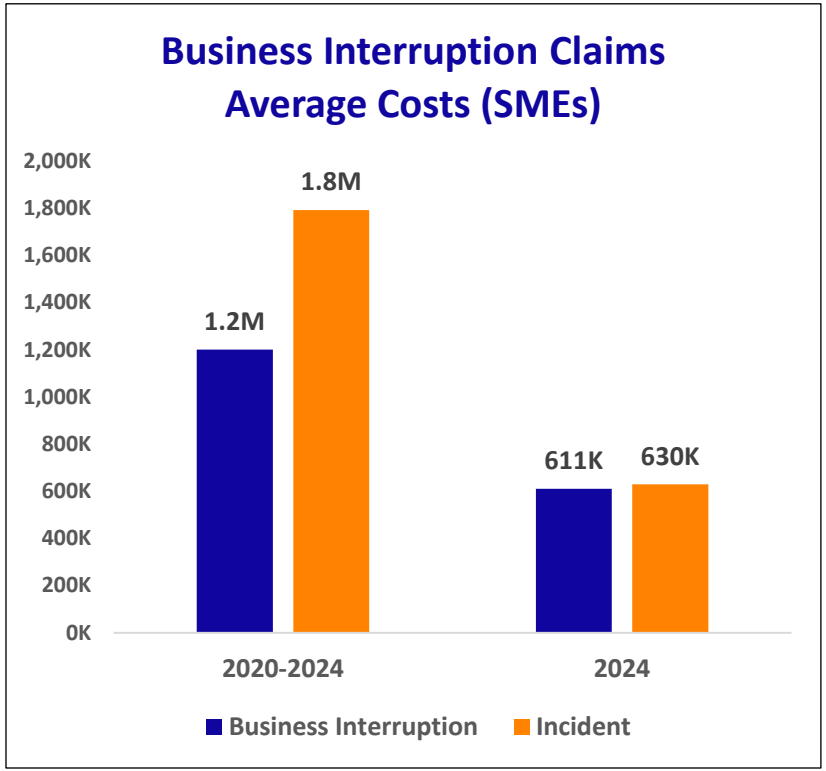
Number of Ransomware Claims by Sector - Top 10

	N=1,934 (75% of Ransomware Claims)			
	Claims	**Payout**	**Total Incident Cost**	**% Claims**
Professional Services	544	474K	520K	21.2%
Manufacturing	326	416K	811K	12.7%
Technology	202	830K	1.4M	7.9%
Healthcare	184	614K	1.4M	7.2%
Retail	176	441K	444K	6.8%
Financial Services	147	759K	890K	5.7%
Education	93	241K	265K	3.6%
Public Entity	90	255K	317K	3.5%
Nonprofit	86	270K	286K	3.3%
Transportation	53	742K	1.2M	2.1%

NetDiligence®

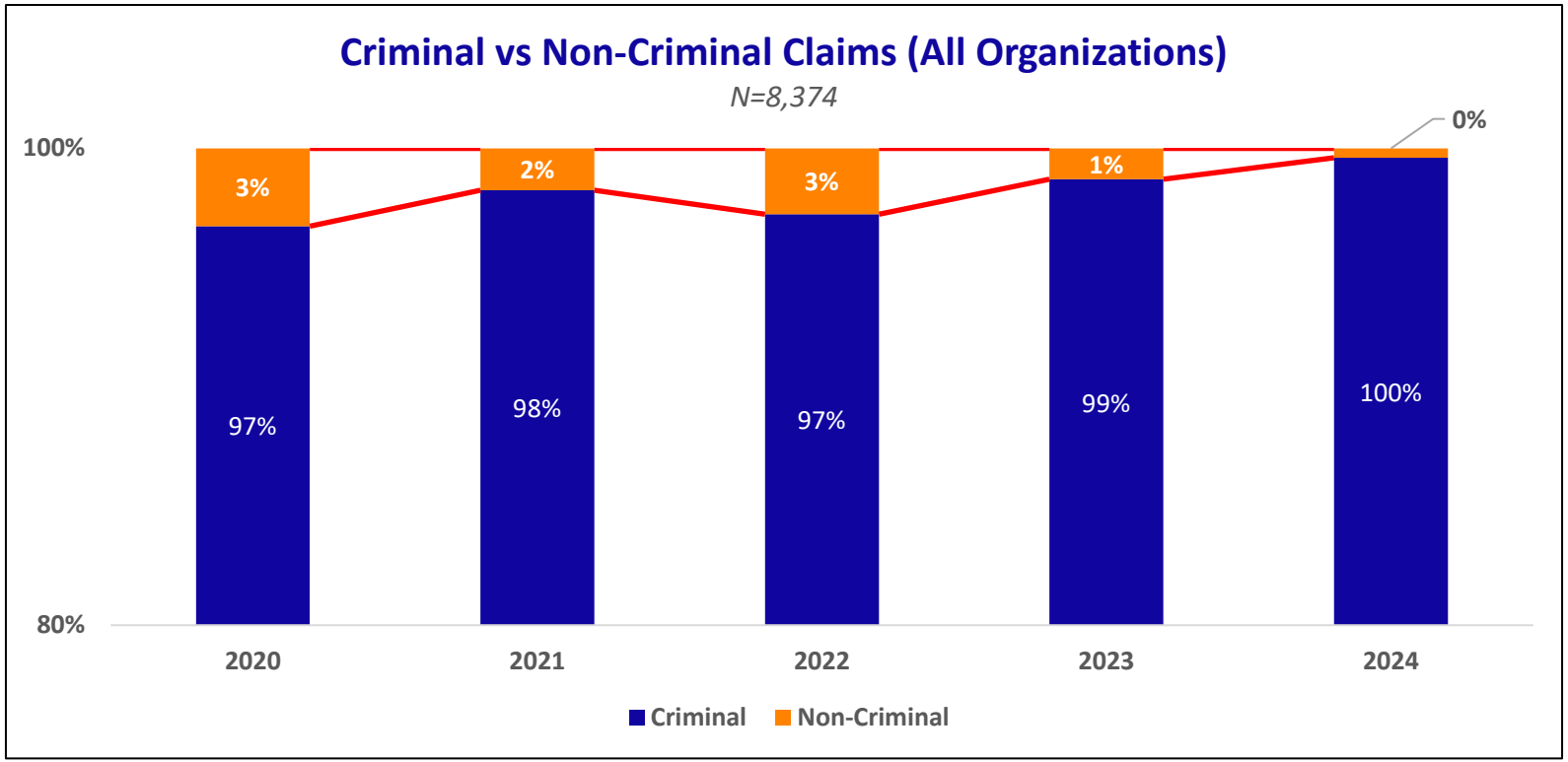
NetDiligence® Cyber Claims Study





NetDiligence®

NetDiligence® Cyber Claims Study



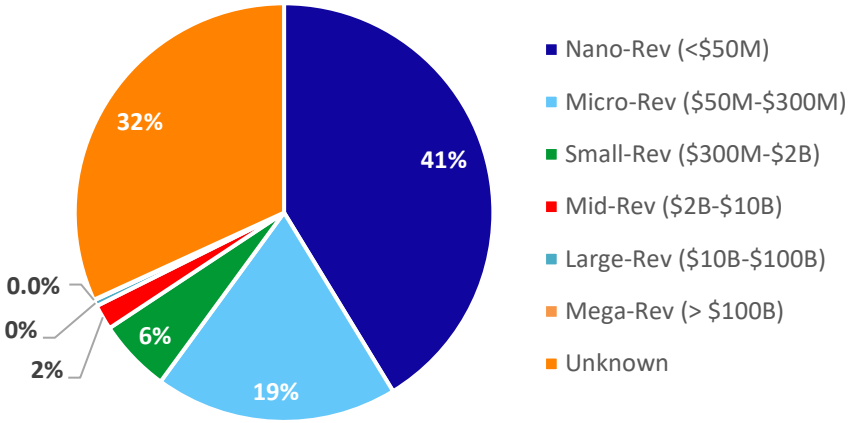
NetDiligence®

NetDiligence® Cyber Claims Study

Percentage of Claims by Organization Size

(All Organizations)

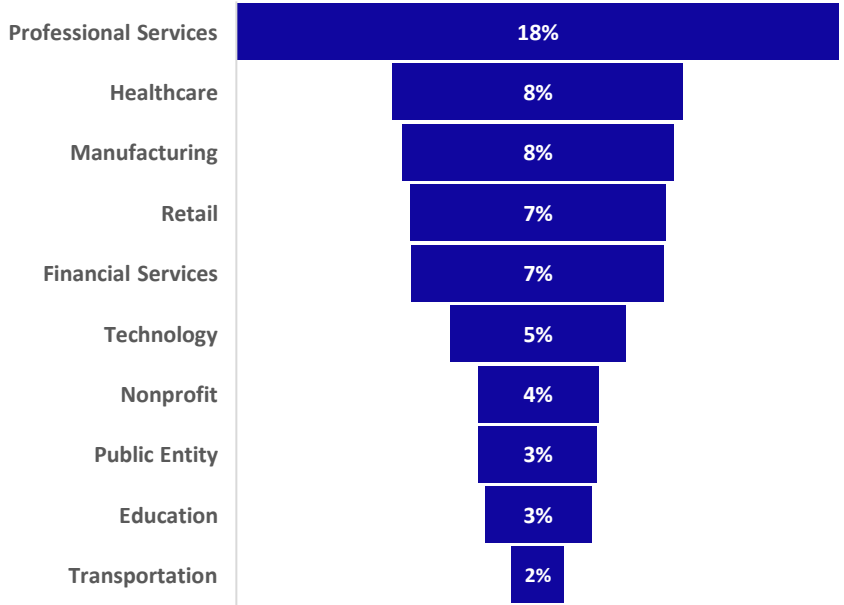
N=10,402



Percentage of Claims by Sector

(All Organizations)

N=10,402



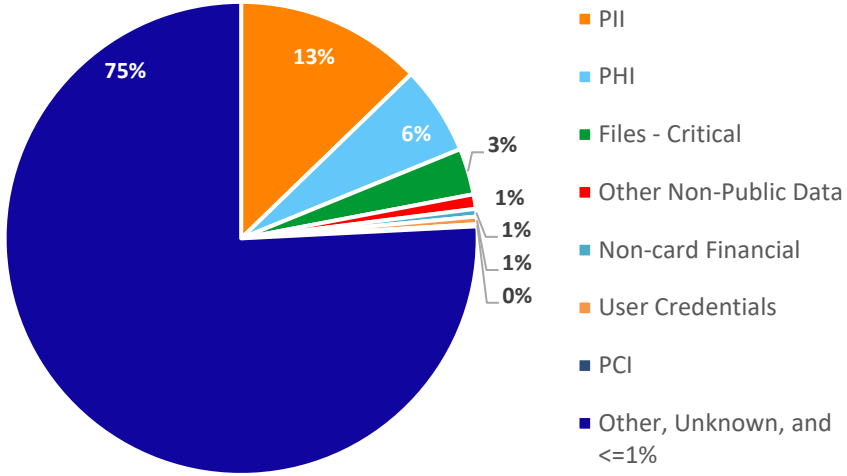
NetDiligence®

NetDiligence® Cyber Claims Study

Percentage of Claims by Type of Data

(All Organizations: 2020-2024)

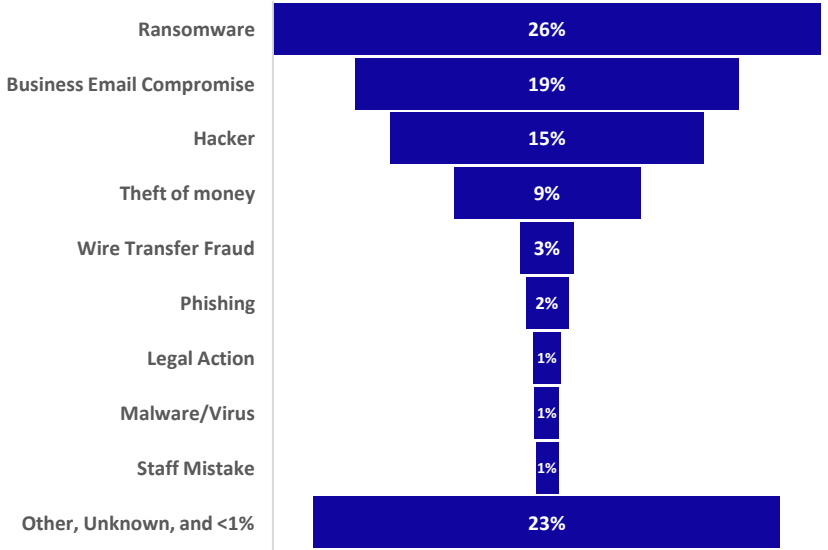
N=10,402



Percentage of Claims by Cause of Loss

(All Organizations)

N=10,402



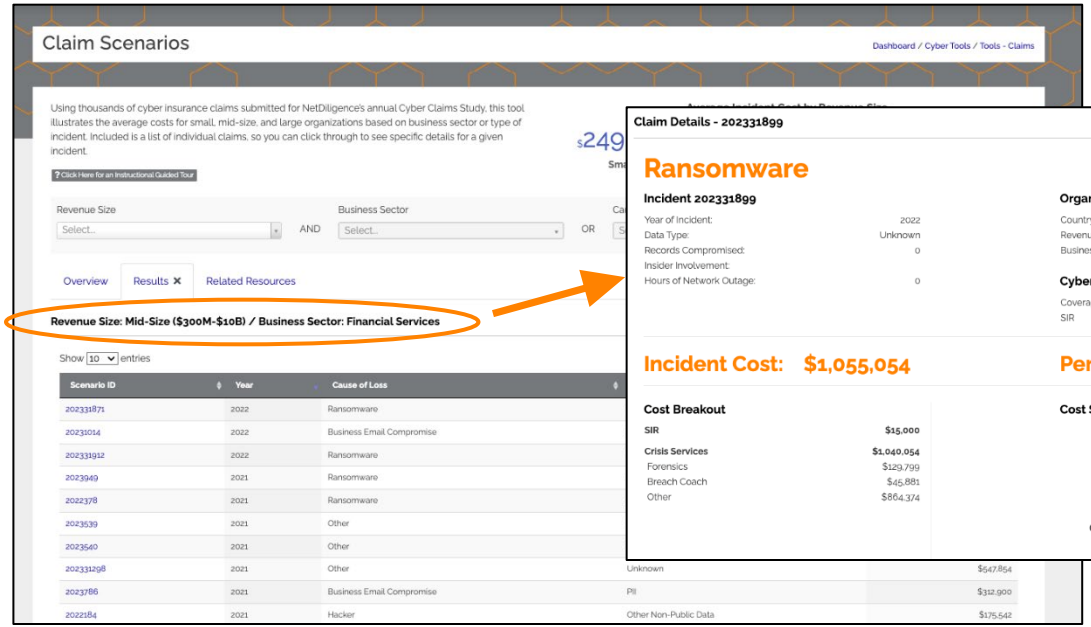
NetDiligence®

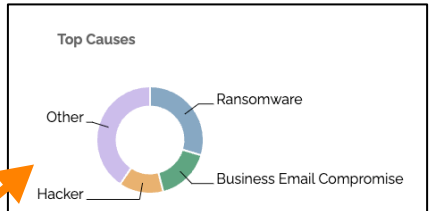
NetDiligence® Cyber Claims Study

Cyber insurance professionals can analyze our latest claims data using the Claim Scenarios tool in eRiskHub®

Available to all users of the eRiskHub, a cyber risk management platform powered by NetDiligence®

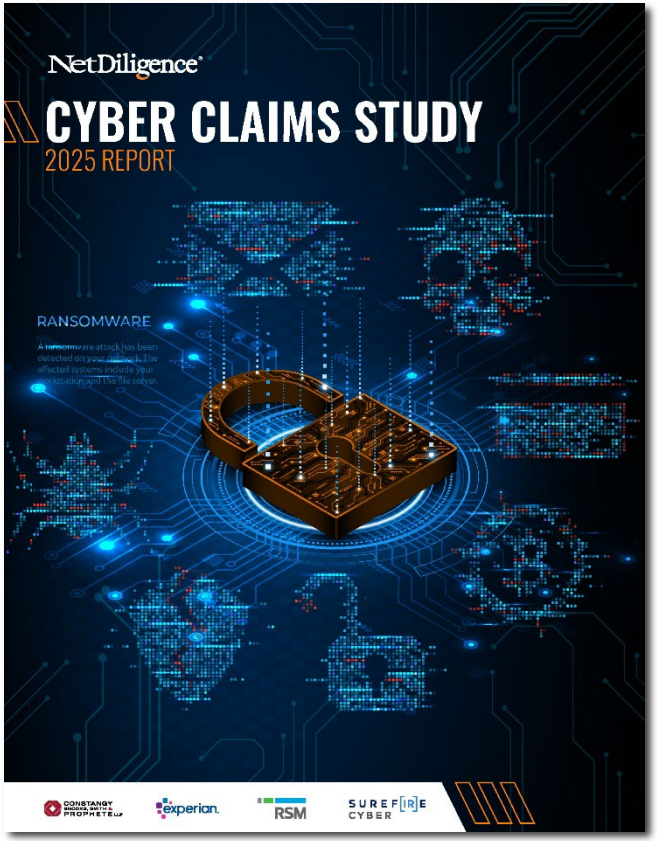
eRiskHub®





NetDiligence®

NetDiligence® Cyber Claims Study



Scan to download the full report

Also available at NetDiligence.com

NetDiligence®

QUESTIONS?