CHUBB®

Navigating the Cyber Claims Landscape

A Guide for Small and Lower Middle Market Businesses

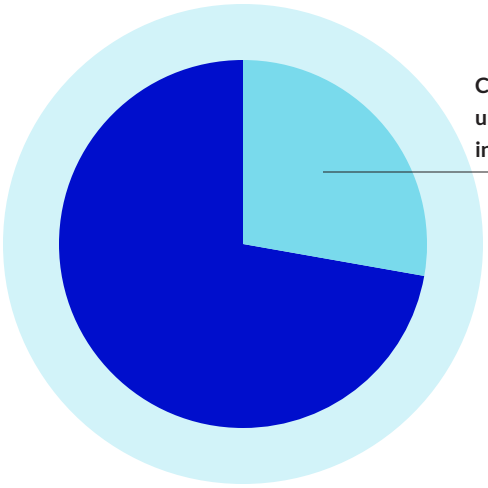
The following guide, based on insights found in the 2025 Chubb report "Navigating the Cyber Claims Landscape," was designed to help small and lower middle market businesses better understand the current threats, identify common cyber risks and institute proactive measures to protect themselves.

Cyber Threats: Recent Trends Affecting Small and Lower Middle Market Businesses

Recent advances in technology, including the rapid and global rise of artificial intelligence and cloud computing, have made businesses of all sizes more vulnerable to both malicious cyber activity and non-malicious causes of system failure. The Chubb report reveals that while incidents involving larger organizations typically make headlines, smaller businesses are by no means immune. More than half of Chubb's 2024 cyber claims originated from companies with under $150 million in annual revenue, while 28% of them impacted businesses with under $25 million in revenue.

Cybercriminals are increasingly targeting small and middle market businesses. A 2024 report from Microsoft revealed that one in three of these businesses has been the victim of a cyberattack, and that such attacks end up costing these companies more than $250,000 on average – and up to $7 million in some cases. Though awareness of cyber risk is growing among all enterprises, data suggests that smaller businesses may not be implementing protective measures at the same rate as their larger counterparts.

Chubb's 2024 Cyber Claims



The Smaller the Company, the Greater the Vulnerability

Though the leaders of some smaller businesses may think the size of their operation makes them less attractive of a target for cybercriminals, these organizations may actually be at a disproportionately higher risk for several reasons:

- **Limited budgets:** Smaller businesses are less likely to have the financial resources available to create and maintain dedicated IT or cybersecurity teams.

- **Limited expertise and/or technology:** Relatedly, employees tasked with monitoring and reducing cybersecurity risks at these companies may not have the specialized experience or tools that allow them to effectively identify weaknesses and conduct regular security assessments.

- **A broader threat landscape:** These businesses may be targeted by cybercriminals precisely because they are perceived to have fewer resources and less-robust security measures in place.

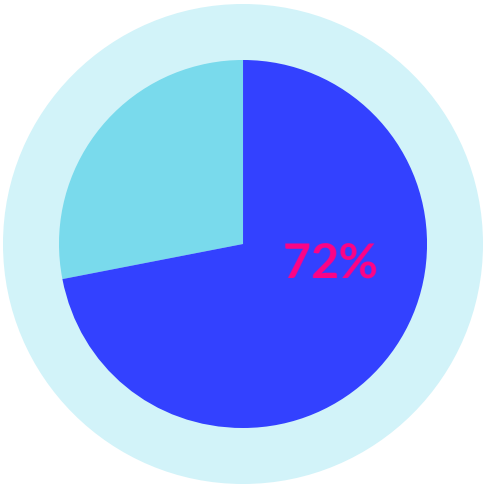
While the smaller size of these companies may signify increased vulnerability, it may also signify a decreased chance for financial and/or reputational recovery in the wake of a serious cyber incident.

Ransomware: A Pervasive Threat

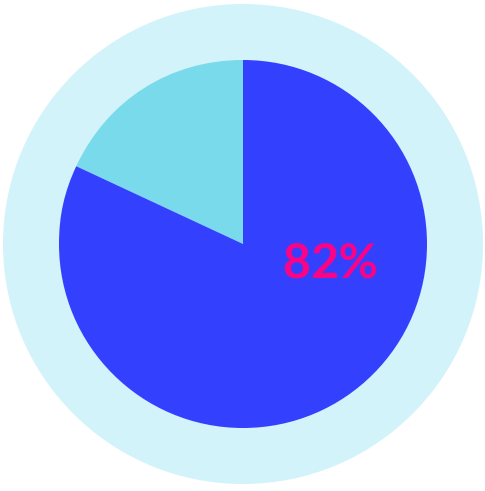
Globally, ransomware attacks remain the chief driver of cyber insurance loss severity. These attacks involve threat actors demanding money to restore access after encrypting an organization's data and/or preventing the dissemination of personally identifiable information. Chubb's report shows that such incidents accounted for nearly 72% of cyber claims dollars in 2023 - 2024. Additionally, third-party litigation stemming from ransomware incidents in the U.S. was up approximately 75% in 2024 compared to the 2020 - 2021 average.

According to the University of Maryland's Francis King Carey School of Law, 82% of ransomware attacks target small to medium-sized businesses. Though ransomware attacks are a significant concern for businesses of all sizes, for a small or lower middle market business they can be catastrophic, as many of these attacks can lead to significant financial losses resulting from downtime and data recovery efforts, in addition to ransom payments and subsequent liability costs related to a data breach.

Percentage of Chubb cyber claims connected to ransomware incidents (2023-2024)



Percentage of ransomware attacks targeting small to medium-sized businesses

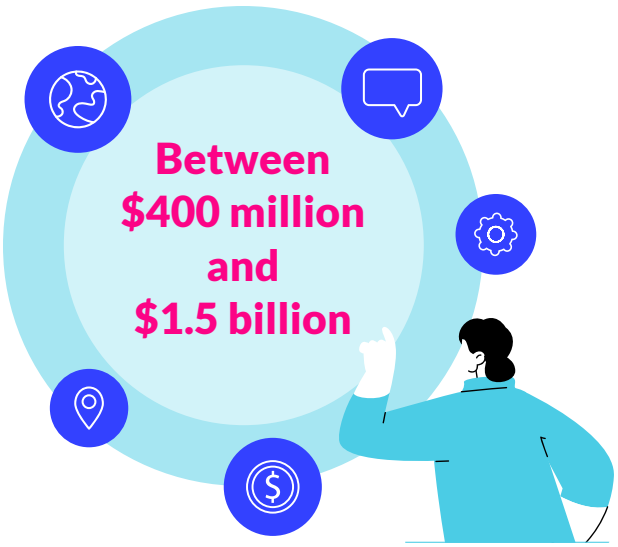


Risks from Non-Malicious Sources

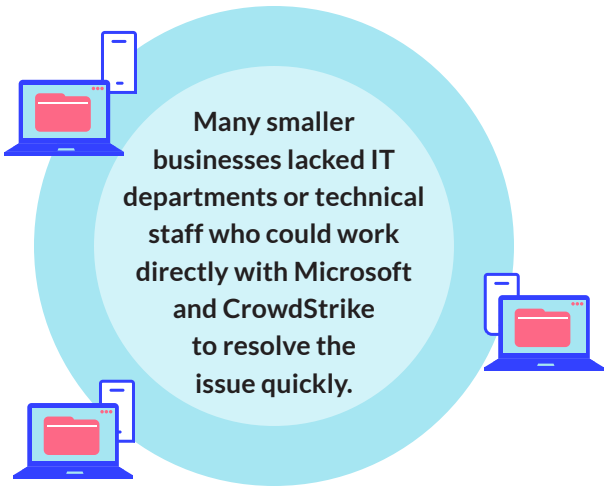
Although malicious cyberattacks tend to receive the most media attention, non-malicious cyber events, often attributable to human error or flawed software design, can be just as damaging. A recent example is the CrowdStrike outage of July 2024, which was caused by a faulty software update. This single event resulted in global disruption, leading to tens of thousands of businesses being unable to function. Insured losses from the incident were estimated to be between $400 million and $1.5 billion.

Airlines, hospitals, financial institutions and other large enterprises were impacted by the CrowdStrike outage, but smaller businesses were negatively affected as well. Any computer or device that ran on Microsoft Windows and received the infected software update crashed and was unable to restart without great effort. Many of the 8.5 million impacted computers and devices belonged to smaller organizations; retailers, medical offices, restaurants and locksmiths all reported experiencing problems accessing essential data, including data relating to payments and shipments. Unlike their larger counterparts, many smaller businesses lacked IT departments or technical staff who could work directly with Microsoft and CrowdStrike to resolve the issue quickly. For a large number of them, the outage – and the associated business interruption – lasted much longer.

Insured losses from 2024 CrowdStrike outage



Impacted computers and devices



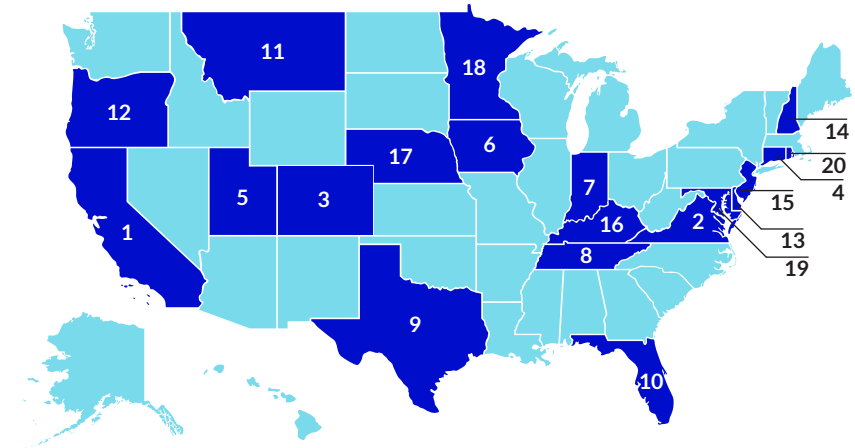
The Growing Impact of Privacy Laws

Another area of rising concern for businesses of all sizes is privacy-related liability. As governments worldwide pass new laws regulating personal and biometric data, the risk of litigation has increased accordingly. Chubb data reveals that the proportion of third-party claims related to privacy liability in the U.S. more than doubled in 2023-2024 when compared to 2020-2022. Laws such as Illinois' Biometric Information Privacy Act (BIPA), the Video Privacy Protection Act (VPPA) and various state wiretapping statutes are leading to this rise in claims.

Many smaller businesses don't have legal or regulatory experts on staff who are able to keep up with this rapidly expanding body of law and ensure compliance. Violations, however, can lead to major consequences; the VPPA, for example, allows for statutory damages of up to $2,500 per violation for unauthorized disclosure of personal information and viewing history. In addition to fines and penalties, small and lower middle market businesses may face lawsuits from individuals claiming harms as a result of data breaches emanating from a lack of due diligence. These smaller companies will likely have more difficulty than larger ones in dealing with these consequences. Additionally, these companies may face reputational damage that can harm business relationships and erode customer trust – ramifications that almost definitionally have a disproportionate impact on smaller businesses.

As of this writing, 20 U.S. states currently have or will soon have privacy laws in effect that create liability for businesses that collect and store personal information. Important to remember is that these laws apply to the state where a plaintiff resides, not where the business is located – a fact that significantly expands the liability risk for companies with clients or customers in multiple states. Different jurisdictions define the term "violation of privacy" differently; businesses that buy or sell customer databases for sales or marketing purposes, for example, should fully understand how these laws can open them up to liability.

States that currently have or will soon have privacy laws that impact liability



1	California	11	Montana
2	Virginia	12	Oregon
3	Colorado	13	Delaware
4	Connecticut	14	New Hampshire
5	Utah	15	New Jersey
6	Iowa	16	Kentucky
7	Indiana	17	Nebraska
8	Tennessee	18	Minnesota
9	Texas	19	Maryland
10	Florida	20	Rhode Island

Encouraging Action and Vigilance

Effective cyber resilience calls upon organizations of all sizes to take simple yet highly effective actions to protect themselves. Among them:

- **Adopt a zero-trust security model.** These models minimize the risk of breaches by requiring stringent identity verifications for anyone seeking to access a private network, irrespective of their location or their status within the organization. Chubb's report highlights the fact that multi-factor authentication (MFA), a core component of a zero-trust model, can significantly reduce risk. Other aspects of the model might include least-privilege access and network microsegmentation.

- **Practice good cyber hygiene.** Companies with strong security controls and resilience capabilities are better able to mitigate the impact of cyber threats. Regular training for employees is crucial, as many attacks don't stem from sophisticated malware but rather rely on social engineering tactics, such as SIM swaps or the manipulation of IT help desks. For 2025, NCSAM is promoting four key actions: using strong passwords, turning on MFA, identifying and reporting scams and updating software.

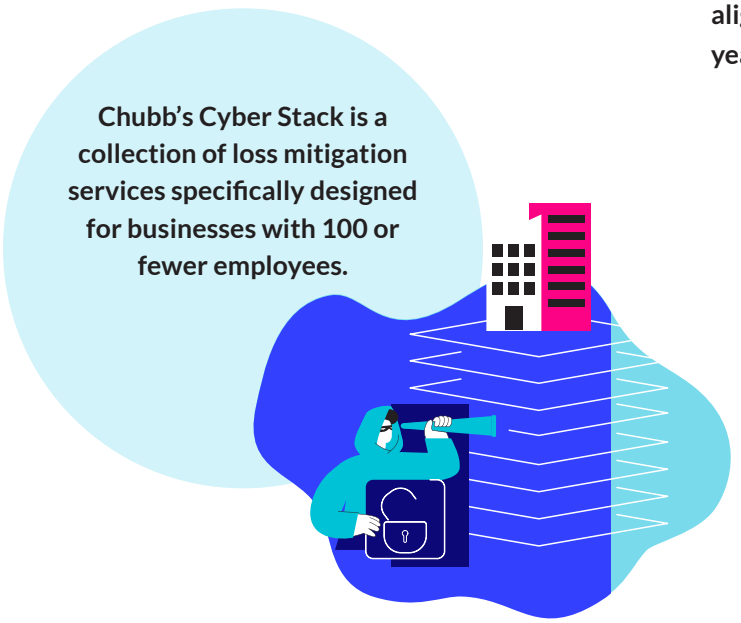
- **Prepare and plan.** Having a solid incident response plan in place is essential for cyber resilience. This includes rehearsing what to do in the event of an attack and ensuring you have robust offline backups to recover critical data. Chubb's report notes that clients outside of the U.S. who have invested in business continuity and incident response plans have seen decreases in both the frequency and severity of cyber incidents.

- **Consider a cyber insurance policy.** While a strong security posture is your first line of defense, cyber insurance can provide a crucial safety net. The right policy can cover financial losses and legal fees while at the same time providing access to expert incident response services.

Chubb's Tailored Initiatives for Smaller Businesses

Recognizing the unique challenges faced by small and lower middle market businesses, Chubb offers these clients a full suite of innovative cyber insurance solutions and risk management services at discounted prices or even at no additional cost. They include:

The Chubb Cyber Stack: A collection of loss mitigation services specifically designed for businesses with 100 or fewer employees. This program connects you with Chubb's team of dedicated cyber risk advisors and provides tools to help you craft effective management and response strategies. Services – which are included at no additional cost for the first year for net new customers to the vendor, with a cost savings benefit of up to $28,000 – include cyber awareness training, vulnerability security alerts, password management and incident response planning.



The Chubb Cyber Index: An externally facing claims database that allows users to access proprietary Chubb data on cyber threats to inform their cyber resilience strategies. This is particularly valuable for the lower middle market segment, as it allows businesses to benchmark their risk profiles against peers, examine peer purchasing insights and use a cyber risk calculator to understand potential exposures and costs.

By taking proactive steps and remaining vigilant, you can significantly strengthen your company's resilience in the face of a costly or damaging cyber incident, aligning your business with the core message of this year's NCSAM: Building a Cyber Strong America.

CHUBB®